**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

# ОСНОВИ ІНФОРМАЦІЙНОГО ПРАВА

## Навчальний посібник

**Київ-2015**

**УДК 343.346.8**
**ББК 67.99**
**О-75**

*Рекомендовано Вченою радою Національного технічного університету України «Київський політехнічний інститут» (протокол №6 від 15.10.2014 р.)*

**Рецензенти:**
- **Новицький А.М.,** доктор юридичних наук, начальник Науково-дослідного центру з питань оподаткування Національного університету державної податкової служби України;
- **Калюжний Р.А.,** доктор юридичних наук, член Міжнародної Академії інформатизації, академік Академії наук Вищої освіти України.

**О-75 Основи інформаційного права:** навчальний посібник / укл. Л.В. Борець, А.Ю. Нашинець-Наумова; за ред. І.П. Голосніченка. – К.: Вид-во «Сталь».- 2015.-98 с.

Інформаційне право як наука динамічно розвивається, його основні положення перебувають у стадії формування. Основна задача навчального посібника на основі аналізу законодавства, практики його застосування в доступній формі подати основні положення щодо предмету, принципів, методів правового регулювання, суб'єктів правовідносин, пов'язаних з інформацією тощо.

Навчальний посібник розраховано на науковців, викладачів, аспірантів, студентів вищих навчальних закладів.

**УДК 343.346.8**
**ББК 67.99**

**ЗМІСТ**

# ВСТУП

Сьогодні високі інформаційні технології буквально пронизують наше суспільство. В умовах розвитку ринкової економіки вони набувають особливого значення, оскільки дозволяють здійснювати управління державою не адміністративними методами, а соціально орієнтованими. Обов'язковими передумовами побудови правової держави, створення демократичної та ефективної системи управління справами країни, формування передової соціально орієнтованої економіки, піднесення нації, освіти, культури – це інформаційний потенціал, який відповідає найсуворішим мірилам науково-технічного прогресу. Високі інтелектуальні технології в сфері інформатизації перетворюються на сильний фактор, який активно впливає на розвиток людства. Належний стан інформаційної справи підвищує рівень правової захищеності людини. Нові технології сприяють розширенню прямих і зворотних зв'язків між державою і громадянським суспільством.

Сама по собі інформатизація нейтральна, але вона створює сприятливі умови для проведення структурних державних реформ. Розширення сфери інформаційної діяльності, розвиток інформаційних технологій зумовили появі такої галузі законодавства, як інформаційне право. У багатьох країнах світу вчені заявляють про створенні самостійної галузі права – інформаційного права. Стан інформаційного права відображає роль і місце інформатизації в житті країни, ставлення до неї з боку влади і всього суспільства. Будучи значною мірою зумовлене обсягом, характером і призначенням всієї інформаційної справи, само інформаційне право, в свою чергу, впливає на хід інформаційних процесів.

В інформаційному праві ми знаходимо величезну кількість теоретичних і практичних невирішених проблем. Це пов'язано в першу чергу з браком фахівців у даній сфері. Поглиблене вивчення інформаційного права необхідно не тільки юристам, а й величезній армії державних службовців. Сучасна

держава активно поширює використання новітніх технологій, що дозволяє наблизити державний апарат конкретним людям.

Термінологія інформаційного права досі значною мірою не відпрацьована, хоча останнім часом вченими проведена велика робота в цьому напрямку. Розслідування інформаційних правопорушень, їх профілактика неможливі без уніфікації підходів в теорії інформаційного права.

Цей навчальний посібник є відносно коротким викладом науково-теоретичного матеріалу з усіх тем навчального курсу. Деякі теми викладаються в посібнику вельми фрагментарно. Це можна пояснити. По-перше, сучасне інформаційне законодавство включає в себе величезну кількість важливих і необхідних для пізнання студентами законів та інших нормативних правових актів. Цей факт не дозволяє детально розглядати в посібнику дані та інші інформаційно-правові інститути. По-друге, автори підручника рекомендують для вивчення відповідні нормативні правові акти, в яких містяться норми, регулюючі відповідні управлінські відносини. Уважне ознайомлення з текстами рекомендованих законів дозволить студентам всебічно вивчити навчальний матеріал. Студентам рекомендується, ґрунтуючись на загальних уявленнях про сутність тієї чи іншої теми, самостійно аналізувати відповідні закони та інші нормативно-правові акти, рекомендовані для вивчення інформаційно-правовими інститутами.

## Розділ І Основні положення інформаційного права

## Тема 1. Предмет інформаційного права та його принципи. Методи інформаційного права.

### 1.1 Правова природа інформаційного права в Україні

За правовою природою інформаційне право - це складова підсистема в системі національного права України, що має приватноправову і публічно-правову природу. Норми інформаційного права формуються як на публічному (державному), так і приватному рівнях суспільних відносин щодо інформації у ході різноманітної діяльності людей.

Інформаційне право через предмет правовідносин - інформацію пов’язане як з провідними галузями права (конституційним, адміністративним, цивільним, кримінальним) так і з різними іншими комплексними галузями права (фінансовим, господарським, екологічним ін.), спеціальними галузями права (інвестиційним, транспортним, повітряним, податковим, бюджетним, банківським, страховим, конкурентним та ін.), а також міжгалузевими інститутами права: правом інтелектуальної власності ( у його складі - авторським, винахідницьким тощо), з іншими інститутами різних галузей права, де похідним предметом є суспільні відносини щодо інформації (твір, винахід, корисна модель, масова інформація, архіви, бібліотеки тощо). Субінститутами інформаційного права можна вважати такі, як: право свободи інформації, право доступу до інформації, правовий режим інформації з обмеженим доступом та інші.

Структурно сучасне інформаційне право має три частини: загальну, особливу і спеціальну. У загальній частині визначаються основні положення щодо мети, завдань, принципів, змісту, суб'єктів правовідносин, пов’язаних з інформацією тощо. У особливій частині визначальними є чотири провідні інститути: права та обов'язки людини, громадянина пов'язані з інформацією; права суспільства, громадських формувань у соціальній інформаційній сфері; права та обов’язки держави в суспільній інформаційній сфері, основні засади

міжнародного співробітництва країни у глобальному інформаційному просторі. У спеціальній частині визначальним є структуризація правовідносин в суспільній інформаційній сфері за напрямками діяльності: мас - медіа право, інформатизаційне право, право інформаційної безпеки, Інтернет-право, телекомунікаційне право тощо.

Категорія «інформаційне право» може розглядатися в кількох розуміннях:

- як галузь права, тобто сукупність юридичних норм (правил поведінки), що регулюють суспільні відносини в сфері обігу інформації;
- як суб'єктивне право, що характеризує можливість для суб'єктів інформаційних відносин вільно одержувати, використовувати, поширювати та зберігати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій;
- як наука, тобто область юриспруденції, що вивчає інформаційне законодавство (право), практику його застосування, досліджує проблеми вдосконалення інформаційно-правових норм;
- як навчальний курс, що пов'язаний із викладанням науки інформаційного права, який висвітлює питання визначення поняття інформаційного права та предмету його регулювання, з'ясовує його завдання, місце в системі права, історичні питання формування цієї галузі та окремих її інститутів, включає питання теоретичних концепцій (шкіл) інформаційного права та питання інформаційного права іноземних держав тощо.

### 1.2. Поняття, предмет, принципи інформаційного права

*Поняття "інформаційне право"* з'явилося порівняно недавно і трактується різними вченими юристами по-різному. Однак в основу всіх визначень покладено принцип предметної галузі інформаційного права, по відношенню до якого або у зв'язку з яким виникають суспільні відносини, що підлягають правовому регулюванню.

В інформаційному праві основним *об'єктом*, з приводу якого виникають суспільні відносини, що підлягають правовому регулюванню, є *інформація*, що

знаходиться в цивільному, адміністративному або іншому громадському обороті.

**Інформаційне право** - система правових норм, що регулюють на комплексній основі дозволів і заборон суспільні відносини з пошуку, накопичення, передачі, виробництва та розповсюдження інформації та похідних від неї продуктів.

Чимало дискусій точиться навколо питання, чи можна відносити "інформаційне право" до самостійної галузі права? Розглянемо це питання детальніше.

Право, виконуючи економічні і соціально-політичні функції і взаємодіючи з державою в особі уповноважених на правотворчість органів, постійно розвивається, удосконалюється і змінюється. Це слід пов'язувати з різноманітними стратегічними завданнями і цілями, які ставляться в той чи інший історичний період. Право як єдина система правил поведінки, регулює суспільні відносини, що різняться за об'єктом, змістом, суттю, суб'єктним складом і іншими критеріями. Зазначена позиція передбачає поділ системи права на галузі та інститути.

В свою чергу, під галуззю права слід розуміти відокремлену в середині певної системи сукупність правових норм, що регулюють певну сферу суспільних відносин. Об'єктивна необхідність сприяє виділенню галузі права. Законодавець лише усвідомлює і намагається оформити цю потребу.

Зважаючи на те, що особливої актуальності на сьогодні набули проблеми формування інформаційного суспільства, стрімко зросла кількість спеціалістів, зайнятих в цій сфері: у суспільстві виникають процеси трансформації багатьох державно-правових інститутів у зв'язку з підвищенням соціальної ролі інформації і розвитком глобальних мереж. Постають нові правові проблеми, пов'язані з використанням глобальних інформаційно-комунікативних систем в інфраструктурі ресурсів економіки, політики, інших соціальних сфер. Під впливом цих факторів формується особлива, комплексна галузь права –

інформаційне право. Це не лише виділення особливої структури в системі комплексних галузей, а й відображення процесу значних змін в уже сформованих галузях права і законодавства.

У науковій літературі останніх років можна виділити цілий спектр понять, за допомогою яких автори намагаються назвати цю нову галузь права. До таких термінів можна віднести: “програмне право”, “програмна інформатика”, “право інформатики”, “комп‘ютерне право”, “інформаційно-комп‘ютерне право”, “право знати”, “право на доступ до інформації”, “право на інформацію”, а також “телекомунікаційне право” і “інформаційне право” (див. роботи А.Б. Агапова, Ю.М. Батурина, І.Л. Бачило, А.Б. Венгрова, М.М. Рассолова, Ю.А. Тихомирова і інших).

В.А. Копилов у своїх працях зазначає, що всі вищезазначені терміни можна поділити на дві групи. Терміни першої групи, швидше за все, виникають завдяки об‘єктам, у зв‘язку з якими виникають суспільні відносини (це програми для ЕОМ; комп‘ютери; інформатика як наука, що вивчає інформацію; одночасно “інформація” і “комп‘ютери” як пов‘язані поняття; телекомунікації як засіб отримання, передачі і знищення зв‘язку. Друга група термінів базується на застосуванні понять, що уособлюють інформаційні права та свободи, що мають гарантуватись інформаційним правом, - “право знати”, “право на доступ до інформації” та ін.

Не зважаючи на різноманітність цих понять, всіх їх можна об‘єднати в один клас через поняття “інформаційна сфера” (сфера діяльності, пов’язана із створенням, поширенням, перетворенням і використанням інформації), в якій вони застосовуються або як її складові частини, або як асоційовано пов‘язані з нею. Вважаємо, що інформаційну сферу слід розглядати в сукупності, а не зупинятись на її окремих складових – інформатика, програмні засоби, комп‘ютери, їх системи, засоби зв‘язку, телекомунікації та ін.

На думку деяких науковців, повноцінність галузі права може бути визначена при наявності трьох її складових, а саме: 1) самостійності предмета і

метода відносно інших галузей права; 2) самостійність нормативно-правової основи галузі, достатньої для формування окремої галузі законодавства; 3) самостійність її доктрини і навчальної дисципліни.

Під предметом інформаційного права слід розуміти інформаційні відносини як відокремлену групу суспільних відносин, що виникають у процесі обігу інформації в інформаційній сфері в результаті здійснення інформаційних процесів у порядку реалізації кожним інформаційних прав і свобод, а також в порядку виконання обов‘язків органами державної влади і місцевого самоврядування щодо забезпечення гарантій інформаційних прав і свобод.

Проблематичним залишається питання про самостійність методу даної галузі права. Не зважаючи на явно виражену самостійність предмету правового регулювання, інформаційне право не може мати власного методу, на зразок цивільного чи кримінального права, оскільки є комплексною галуззю. Тут реалізуються методи усіх класичних галузей права: конституційного, адміністративного, цивільного і кримінального. За цією ознакою інформаційне право є галуззю другого рівня, що реалізує методи базових галузей права, що не заважає розвитку її теоретичної і нормативної основи.

Два інші індикатора для галузі інформаційного права – наявність законодавства і навчальних курсів з окремих напрямків і всього комплексу проблем себе вже проявляють. За останні роки сформовано значний масив українського законодавства і прийнято велику кількість підзаконних актів, які регулюють різноманітні напрямки діяльності в інформаційній сфері.

Таким чином, є підстави для виділення інформаційного права в нову комплексну галузь права, яку слід розглядати як сукупність однорідних правових норм, які регулюють суспільні відносини, що виникають в інформаційній сфері.

*Предметом інформаційного права* є суспільні відносини, які пов'язані зі створенням, формуванням, зберіганням, обробкою, поширенням, використанням та утилізацією інформаційних продуктів, наданням

інформаційних послуг, управлінням процесом формування й використання інформаційного продукту та надання інформаційних послуг, розвитком і застосуванням нових технологій роботи з інформацією та її передавання в системах і мережах комунікацій, посиленням безпеки в інформаційній сфері, а також з юридичною відповідальністю суб'єктів права у цих відносинах.

*Принципи* інформаційного права – це основоположні ідеї, що визначають його сутність і зміст. Умовно принципи інформаційного права можна поділити на загальні і спеціальні.

До загальних слід віднести принципи законності, вільного доступу до інформації, вільного висловлення думок і переконань, забезпечення інформаційної безпеки, рівності громадян на отримання інформації, захисту авторських прав та ін.

До спеціальних належать такі принципи, як право на приватну інформацію, точне дотримання правил користування інформаційними ресурсами, технологіями, системами, недоторканність інформації про приватне життя, дотримання норм авторського права, доступність відкритої інформації тощо.

Класифікувати принципи інформаційного права можливо й за іншими критеріями. Зокрема, залежно від сфери застосування принципи можна класифікувати на загальноправові, міжгалузеві й галузеві.

Проаналізуємо основні принципи:

1. Принцип законності - суб'єкти інформаційного права зобов'язані суворо дотримуватися Конституції України, органи державної влади зобов'язані захищати права і свободи людини і громадянина в інформаційній сфері.

2. Принцип вільного виробництва і розповсюдження будь-якої інформації, не обмеженої законом.

3. Принцип заборони виробництва і розповсюдження інформації шкідливої і небезпечної - заборона спрямований на захист інтересів і свобод

особи і суспільства від впливу шкідливої інформації. Заборона може накладатися тільки законодавчо.

4. Принцип вільного доступу до не обмеженої законом інформації. Жодна державна структура не може вводити обмежень з доступу споживачів до інформації, якою вона володіє відповідно наданої їй компетенцією, яка зачіпає права і свободи людини і громадянина та представляє суспільний інтерес.

5. Принцип повноти обробки та оперативності надання інформації - означає обов'язок будь-якої державної структури накопичувати, зберігати інформацію в повному обсязі відповідно до встановленої для неї компетенцією, а також надавати у встановлені терміни споживачам.

6. Принцип відповідальності означає невідворотне настання відповідальності за порушення вимог та приписів інформаційно-правових норм.

7. Принцип розповсюдженості інформації означає, що одна і та ж інформація може багаторазово копіюватися в необмеженій кількості без зміни її змісту.

*Функції інформаційного права* можна класифікувати за різними критеріями: (а) за сферою правового впливу на регулятивну, ідеологічну, культурно-виховну; (б) за характером впливу на статичну, динамічну, установчу, інтегративну, охоронну й запобіжну, (в) за сферою, на яку поширюються функції інформаційного права, на галузеву, міжгалузеву, правового інституту, норми права.

Під функцією інформаційного права слід розуміти головні напрями його впливу на інформаційні відносини. Ці напрями обумовлені соціальним призначенням інформаційного права. Характеристику інформаційного права доповнюють перелік його функцій і внутрішня система побудови.

Вплив інформаційного права здійснюється через свідому належну або можливу поведінку людей. Він є проявом динаміки інформаційного права і реалізується через виконання суб’єктом права своїх прав і обов’язків.

Функції інформаційного права безпосередньо спрямовані на виконання завдань, що стоять перед суспільством. Слід розрізняти економічні, політичні, культурні, виховні, інформаційні, екологічні та інші функції інформаційного права.

Щодо власне юридичних функцій інформаційного права, то вони поділяються на регулятивну і охоронну. *Регулятивна функція* інформаційного права спрямована на закріплення суспільних відносин або забезпечення їх розвитку. У здійсненні регулятивної функції інформаційного права особливого значення набуває конституційне закріплення форм власності і основних політичних інститутів, що існують у суспільстві. Інформаційні відносини, таким чином, вводяться інформаційним правом у певні рамки.

Функція правового регулювання може бути спрямована на впорядкування і розвиток інформаційних відносин, на визначення конкретних напрямів поведінки людей, реалізацію ними своїх інформаційних прав і обов'язків. Нині в Україні це набуває особливо великого значення для розвитку ринкових відносин і демократії. Регулятивна функція інформаційного права здійснюється на основі правових приписів і дозволів. Регулювання при цьому може бути загальним, коли регулюється поведінка широкого кола невизначених суб'єктів (наприклад, таємниця інформації про персональні дані) або індивідуальним — коли регулюється поведінка конкретної особи чи вузького кола осіб (наприклад, через рішення, що виносяться судом по інформаційній справі), тобто через акти застосування інформаційного права.

Завданням *охоронної функції* інформаційного права є здійснення впливу на інформаційні відносини шляхом поступового витискування тих явищ, які є небажаними для суспільства. Ця функція здійснюється заради охорони інформації особи і суспільної безпеки з допомогою встановлення заборон та негативних наслідків порушень, шляхів виконання прийнятих щодо правопорушників рішень і т. ін. Слід звернути увагу на дещо умовний характер поділу функцій інформаційного права на регулятивну і правоохоронну. Обидві

функції є проявом однієї властивості інформаційного права — бути регулятором суспільних відносин, бо і при здійсненні охоронної функції інформаційні відносини теж регулюються. В обох випадках йдеться про перетворення нормативності інформаційного права на урегульованість суспільних відносин. Різними лишаються тільки завдання, які виконуються при здійсненні регулятивної і правоохоронної функцій.

Здатність функцій інформаційного права бути регулятором суспільних відносин — головна його корисна властивість і особливість. Саме через наявність цієї властивості право має величезну інструментальну цінність — воно є необхідним і корисним для суспільства феноменом, важливою складовою нормативної основи його життя. Так, згідно зі ст. 3 Конституції України, що визнає людину найвищою соціальною цінністю, права і свободи людини та їх гарантії визначають сутність і спрямованість діяльності держави. Право, регулюючи інформаційні відносини, сприяє правильному поєднанню інтересів особи і суспільства в цілому.

Регулюючи інформаційні відносини, інформаційне право вносить у суспільство організованість, виступає знаряддям організації державного управління, здійснення програмування, соціального контролю тощо. Внаслідок цього право виступає як унікальний феномен, здатний спрямувати розрізнені волі і дії тисяч і мільйонів людей в одному напрямі, перетворюючи їх фактично на єдину волю, що відповідає інтересам суспільства, має загальний характер і покликане забезпечити соціальний прогрес.

### 1.3. Інформаційне право як наука і як навчальна дисципліна

Наука інформаційного права покликана виробляти теоретичні знання шляхом вивчення закономірностей, особливостей та проблем формування і розвитку цієї галузі.

Наука інформаційного права тільки формується, але вже можна виділити найбільш важливі напрямки наукових досліджень, в числі яких:

1. вивчення правових режимів інформації та інформаційних ресурсів;

2. вивчення інформації як об'єкта права;

3. вивчення інформаційних систем, технологій та засобів їх забезпечення;

4. вивчення різних видів режиму закритої інформації;

5. дослідження структури інформаційного права як комплексної галузі права;

6. дослідження практики застосування норм інформаційного законодавства;

7. вивчення правових проблем глобальної мережі Інтернет;

8. вивчення правових проблем інформаційної безпеки.

Наведений перелік не є вичерпним, так як сфера інформаційних відносин активно розвивається, формуючи нові напрями наукових досліджень. Тим не менш, наука інформаційного права має фундаментальні теоретичні дослідження.

Інформаційне право як навчальна дисципліна покликана узагальнити основи наукових знань у галузі теорії інформаційного права, розкрити особливості інформаційно-правових норм та інститутів, практику їх застосування, озброїти майбутніх фахівців необхідними для самостійної роботи знаннями і навичками.

**Систему інформаційного права України складає сукупність інформаційно-правових норм та інститутів, об’єднаних принципами й цілями.**

### 1.4. Методи інформаційного права.

*Під методом правового регулювання* розуміють сукупність способів правового впливу на суспільні відносини, що складають його предмет. Особливості методу інформаційного права виявляються у правовому статусі суб'єктів, формі та змісті правових відносин, юридичному інструментарії, який використовується для впливу на суспільні інформаційні відносини. Для регулювання цих відносин застосовуються різні методи публічного та

цивільного права. Їх вибір залежить від виду й призначення інформації, характеру поведінки суб'єктів та відносин, які виникають між ними.

Відомо, що в основу цивільного права покладено метод диспозитивного регулювання з притаманними йому ознаками децентралізації і координації, а публічного - імперативний метод, для якого характерними є централізоване здійснення владних повноважень та субординація суб'єктів правових відносин.

Для інформаційного права характерними є 2 види методів імперативний і диспозитивний. Імперативний метод правового регулювання інформаційних відносин виражається в встановленні для суб’єктів правовідносин заборон, він виключає юридичну рівність сторін, автономію волі суб’єктів. Диспозитивний метод правового регулювання інформаційних відносин забезпечує суб’єктам інформаційних правовідносин рівні права щодо реалізації в межах законодавства своїх цілей і завдань.

**Імперативні методи** - це методи права, які ґрунтуються на нерівності учасників правовідносин і встановлення жорсткої, однозначної моделі їх поведінки.

До імперативним методів належать:

1.метод веління, який полягає у покладанні на учасників інформаційних правовідносин обов'язки вчиняти будь-які дії (наприклад, використання інформації з особливим правовим режимом);

2.метод заборони, який полягає у покладанні на учасників інформаційних правовідносин обов'язку утримуватися від здійснення яких-небудь дій (позначаються діяння, що являють собою інформаційні порушення).

**Диспозитивні методи** - це методи права, які ґрунтуються на рівності учасників правовідносин і на їх можливості самостійно обирати модель можливої поведінки в інформаційному праві.

До диспозитивним методів належать:

1. метод дозволу, який полягає в наданні учасникам інформаційних правовідносин права вчиняти будь-які дії або не робити їх за своїм вибором (частіше використовується у сфері бібліотечної та архівної справи);

2. метод узгодження, який застосовується при регулюванні правовідносин між рівними суб'єктами для досягнення будь-якого згоди між ними (застосовується у сфері інтелектуальної власності);

3. метод рекомендацій, полягає у вказівці законодавцем кращою моделі поведінки учасників інформаційних правовідносин (регулювання засобів масової інформації);

4. метод заохочень, при цьому законодавець надає різні пільги, якщо суб'єкти інформаційного права вибирають запропоновану законодавцем модель поведінки.

В системі інформаційного права: *по-перше*, реалізуються методи конституційного, адміністративного, цивільного, кримінального права і процесуальних норм цих галузей; *по-друге*, використовуються методи міжнародного публічного та приватного права; *по-третє*, зберігають певний ступінь впливу засоби звичайного права і ділових навичок.

Загальна сукупність методів правового регулювання відносин створює особливий правовий режим галузі інформаційного права.

Інформаційно-правовий режим – сукупність загальнообов’язкових правил поведінки громадян та юридичних осіб, а також порядок реалізації ними своїх прав і інтересів в інформаційній сфері, забезпечення інформаційної безпеки й порядку спеціально уповноваженими органами та їх посадовими особами.

Інформаційно-правові режими класифікують: (а) за масштабом волі фізичних і юридичних осіб у використанні своїх можливостей для реалізації прав та інтересів в інформаційній сфері, (б) за часом і територією їх дії, (в) за видами інформації, (г) за видами інформаційної діяльності, (д) за іншими критеріями.

**Контрольні запитання для самоперевірки**

1. Охарактеризуйте правову природу інформаційного права в Україні.
2. Дайте визначення понять «інформаційне право», «предмет інформаційного права».
3. Проаналізуйте основні принципи інформаційного права. Функції інформаційного права та їх завдання.
4. Проаналізуйте інформаційне право як науку і як навчальну дисципліну.
5. Методи інформаційного права.

## Тема 2. Джерела інформаційного права.

### 2.1. Поняття джерел інформаційного права та їх форми.

Джерела інформаційного права – це обставини, що спонукають появу і дію інформаційного права. Термін "джерело інформаційного права" юриспруденції відомий давно. Ще римський історик Тіт Лівій називав закони джерелом особистого і приватного інформаційного права.

**Джерела інформаційного права** України - це прийняті уповноваженими органами акти правотворчості, що повністю складаються з інформаційно-правових норм або містять хоча б одну з них. Особливістю інформаційного права є різноманітність і значна кількість його джерел, що зумовлено тим, що нормами зазначеної галузі регламентується широке коло суспільних відносин. Специфікою таких джерел є те, що всі вони (а) ґрунтуються на Конституції й законах України, (б) приймаються органами виконавчої влади, органами місцевого самоврядування, іншими державними (недержавними) інституціями, (в) мають різну юридичну силу, (г) приймаються одноособово й колегіально, (д) до них належать і деякі міжнародні договори й рішення Конституційного Суду України.

Форма (джерела) інформаційного права – це форма саме інформаційного права як окремого явища, яка співвідноситься тільки зі змістом інформаційного права. Її призначення – впорядкувати інформаційне право, надати йому

властивості державно-владного характеру. Виділяють зовнішню і внутрішню форми інформаційного права.

Під *внутрішньою формою* розуміють систему інформаційного права, що має об'єктивний характер своєї побудови, який виявляється в єдності й узгодженості всіх її норм, диференційованих за правовими комплексами, галузями, підгалузями, інститутами і нормами інформаційного права. Внутрішня форма інформаційного права – це структура і зв'язки. До неї відносять систему інформаційного права, горизонтальну і вертикальну структури співпідпорядкованості всіх її елементів.

*Зовнішня форма* інформаційного права – це спосіб об'єктивізації форми інформаційного права, зовнішнього прояву, матеріальної фіксації. В сучасній науковій літературі різні автори вважають, що поняття інформаційного права відбиває державну волю, а формами інформаційного права виступають інформаційні норми. Проте, на думку більшості науковців, більш близькими до істини є вчені, які поняття інформаційного права визнають не як державну волю (це його сутність), а інформаційні норми, і в цьому зв'язку формою вони називають джерела інформаційного права. Тому інформаційна норма це – не форма інформаційного права, а саме інформаційне право.

**2.2. Зовнішні форми інформаційного права.**

До зовнішніх форм належать:

– інформаційно-правовий прецедент – виражене зовні рішення органу виконавчої влади з конкретної справи, якому надається формальна обов'язковість при розв'язанні наступних аналогічних справ;

– інформаційно-правовий договір – угода двох чи більше суб'єктів інформаційного права про встановлення, зміну або припинення інформаційних прав чи обов'язків;

– інформаційно-правовий акт – письмовий документ компетентного органу держави, в якому закріплено забезпечуване нею формально обов'язкове правило поведінки в інформаційні сфері.

Розглянемо більш детально основні форми інформаційного права.

*Інформаційно-правовий прецедент.* Прецедентом є такі дії влади, що мали місце лише один раз, але можуть бути прикладом для подібних дій цієї влади в подальшому. Інакше кажучи, інформаційно-правовий прецедент – це рішення юрисдикційних органів щодо інформаційно-правової справи, що згодом приймається за загально обов'язкове правило.

Розрізняють судовий та адміністративний прецеденти. При прецедентній формі інформаційного права судові (а іноді й адміністративні) органи фактично наділені правом створювати нові інформаційні норми.

Результатом правозастосувальної діяльності нерідко є створення правових положень, для яких характерний відомий ступінь узагальненості й обов'язковості. Отже, правові положення юридичної практики є прецедентним інформаційним правом.

*Інформаційно-правові договори* – це угода двох чи більше суб’єктів інформаційного права щодо встановлення, зміни або припинення інформаційних прав чи обов’язків. У цих документах міститься волевиявлення сторін із приводу інформаційних прав та обов'язків, визначається їхнє коло і послідовність, а також закріплюється добровільна згода виконувати взяті зобов’язання. Вони мають широке поширення в інформаційному праві.

Для визнання договору джерелом інформаційного права необхідно, щоб він містив інформаційно-правові норми.

Інформаційно-правові договори є проявом нормативної саморегуляції. Але не можна забувати, що первинним юридичним джерелом розвитку договірних форм, надання їм законної сили виступає інформаційно-правовий акт, а конкретніше – диспозитивні норми інформаційного права.

*Інформаційно-правовий акт* – одна з основних, найбільше виражених зовнішніх форм інформаційного права, це державний акт нормативного характеру.

Основним джерелом права більшості сучасних держав є інформаційно-правовий акт. Цим документам властиві певні особливості.

По-перше, вони мають державний характер. Держава наділяє органи, організації, посадових осіб правом приймати інформаційно-правові акти, тобто правотворчою компетенцією. Вона ж забезпечує і реалізацію прийнятих інформаційно-правових актів, включаючи й примусовий вплив на осіб, що ухиляються від їхнього виконання.

По-друге, інформаційно-правові акти приймаються не всіма, а строго визначеними суб'єктами, спеціально уповноваженими на те державою. При цьому кожен суб'єкт правотворчої діяльності має рамки своєї компетенції. Наприклад міністр може видати інформаційно-правовий наказ, але він не уповноважений видавати укази або постанови.

По-третє, ці акти приймаються з дотриманням певної процедури.

По-четверте, вони мають тимчасові, просторові та суб'єктні межі дії.

По-п'яте, завжди містять інформаційні норми. Наявність у цих актах інформаційних норм і робить їх нормативними, загальнообов'язковими.

За юридичною силою всі інформаційно-правові акти поділяються на законодавчі та підзаконні.

*Законодавчі акти* – це акти органу законодавчої влади – Верховної Ради України, які мають найвищу юридичну силу, приймаються в особливому порядку і спрямовані на регулювання основних суспільних відносин. До законодавчих актів, які містять інформаційно-правові норми, відносяться Конституція України, регламент Верховної Ради України, закони України, кодекси та постанови.

*Підзаконні інформаційно-правові акти* – це результат нормотворчої діяльності компетентних органів держави (їх посадових осіб), уповноважених на те державою громадських об’єднань зі встановлення, введення в дію, зміни чи відміни інформаційних документів, що розвивають чи деталізують окремі положення законів.

За суб'єктами видання інформаційно-правові акти, поділяються таким чином:

– Верховної Ради України – закони і постанови;

– Президента України – укази;

– органів виконавчої влади:

- Кабінету Міністрів України – декрети і постанови;
- керівників міністерств та інших центральних органів виконавчої влади – інструкції, вказівки, інформаційно-правові накази;
- місцеві органи виконавчої влади – рішення та інформаційно-правові ухвали;
- адміністрацій державних підприємств, установ, організацій – інформаційно-правові накази.

У деяких випадках нормативного характеру набувають волевиявлення населення в результаті всеукраїнського чи регіонального референдумів, певних громадських об'єднань, трудових колективів, форма яких може бути різною (рішення, постанова і т. ін.).

Інформаційно-правові акти діють у часі, просторі та в певному колі осіб.

При характеристиці дії інформаційно-правових актів у часі слід розрізняти: введення в дію; припинення дії; зворотну силу дії.

Інформаційно-правові акти припиняють свою дію внаслідок: а) закінчення терміну давності, на який видавався акт; б) прямої відміни конкретного акта; в) фактичної відміни акта іншим актом, прийнятим з того самого питання.

Дія нормативних актів у просторі характеризується певною територією:

– держави в цілому;

– відповідного регіону;

– адміністративно-територіальної одиниці;

– відповідного підприємства, організації.

Щодо кола осіб інформаційно-правові акти дійсні для громадян України, осіб без громадянства, іноземних громадян, юридичних осіб.

Крім того, інформаційно-правові акти класифікуються за суб’єктами ухвалення, наприклад: акти органів держави, громадських об’єднань, трудових колективів, спільні акти органів держави та недержавних формувань.

Оскільки основною формою інформаційного права в Україні є інформаційно-правовий акт, то під джерелами інформаційного права слід розуміти зовнішнє вираження інформаційно-правових актів, які приймаються і діють з метою регулювання інформаційних відносин. Різноманітність цих відносин, а також розмежування функцій державних органів припускають наявність численних інформаційних актів. Виходячи з цього, важливе теоретичне й практичне значення має розмежування інформаційно-правових актів за певними критеріями.

Таким чином, інформаційно-правовий акт – це офіційний документ, який створений компетентними органами держави й містить загальнообов’язкові інформаційні норми (правила поведінки).

Інформаційно-правовий акт є результатом діяльності компетентних суб’єктів, яку називають правотворчістю. Це діяльність державних органів і посадових осіб, громадських організацій, уповноважених на те державою, а також усього народу України, яка спрямована на утворення, зміну чи відміну інформаційно-правових актів.

Інформаційно-правові акти – основне джерело інформаційного права не лише в Україні, але й в усіх правових системах світу. Поширеність інформаційно-правових актів пояснюється незаперечними перевагами такого способу вираження інформаційних норм, саме з точки зору загальнолюдських принципів права, які поступово впроваджуються в право.

На відміну від індивідуальних, інформаційно-правові акти мають загальнообов’язковий характер і відрізняються неконкретністю адресата, тобто обов’язкові не для окремої конкретної особи, а для всіх суб'єктів, на яких вони поширюються. Діють інформаційно-правові акти відносно довгий час і не вичерпують себе фактами їхнього застосування.

Інформаційно-правові акти слід також відрізняти від інтерпретаційних актів, тобто актів роз'яснення (тлумачення) норм права. Від інформаційно-правових останні відрізняються тим, що не містять нових інформаційних норм, а лише роз'ясняють існуючі.

Отже, форми (джерела) інформаційного права мають велике значення для зміцнення законності в правовій державі.

**2.3. Інформаційне законодавство.**

Під категорією *інформаційне законодавство* України розуміється сукупність нормативно-правових актів, які регулюють суспільні відносини, пов'язані з обігом інформації. Згідно ст. 17 Закону України "Про інформацію" джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Джерела інформаційного законодавства – це видані державою та визнані нею офіціально-документальні форми вираження та закріплення інформаційно-правових норм.

На думку Г.В. Виноградової, джерела інформаційного законодавства, як комплексної галузі, можуть бути класифіковані на декілька груп:

1. норми Конституції України, що закріплюють інформаційні права та свободи, встановлюють права та обов'язки суб'єктів інформаційних відносин з приводу створення та поширення інформації певного виду, а також встановлюють обмеження в обігу інформації в державі та суспільстві;

2. галузі законодавства, що повністю присвячені питанням регулювання інформаційних відносин. До них належать:

- законодавство про засоби масової інформації;
- законодавство про формування інформаційних ресурсів, створення інформаційних продуктів, надання інформаційних послуг споживачу

(складовими якого, в свою чергу, є законодавство про правову інформацію, законодавство про персональні дані, про бібліотечну справу, про архіви, музеї, про рекламу, про видавничу справу, про статистичну інформацію, законодавство про міжнародний обмін інформацією тощо);

- законодавство про інтелектуальну власність;
- законодавство, що регламентує порядок реалізації права на пошук, отримання, передачу та використання інформації;
- законодавство про створення та використання інформаційних систем, їхніх мереж, інших інформаційних технологій та засобів їх забезпечення;
- законодавство про інформаційну безпеку;

3. інші галузі законодавства, акти яких містять окремі інформаційно-правові норми. Такі норми включаються в такі групи актів:

- нормативно-правові акти, що регламентують правовий статус відповідних органів влади (Конституція України, конституційні та звичайні закони, які визначають компетенцію органів державної влади, в тому числі щодо формування та використання державних інформаційних ресурсів);
- нормативно-правові акти цивільного законодавства, в яких отримують розвиток питання реалізації права власності на інформацію, в тому числі питання укладання, виконання та розірвання договорів на одержання та використання інформації;
- нормативно-правові акти, що регулюють відносини в різних галузях господарської діяльності (зокрема, законодавство про землю, про надра, про охорону природи тощо). Адже різні види господарської діяльності і супроводжуються створенням інформації певного виду та призначення, що включається в господарський обіг;
- нормативно-правові акти про відповідальність за правопорушення в інформаційній сфері.

Однак, зважаючи на зміст загальної теорії права та спираючись на положення Закону України „Про інформацію”, необхідно доповнити зазначений перелік джерел ще декількома групами:

- міжнародні нормативно-правові акти, що декларують інформаційні права людини, встановлюють обмеження щодо отримання та використання інформації про особу, що присвячені питанням дотримання промислової, комерційної таємниці, встановлення принципів рекламної діяльності тощо;
- міжнародні угоди у галузі здійснення інформаційної політики.

**2.4. Міжнародно-правові стандарти в сфері інформаційного права.**

За останні роки було ухвалено міжнародно-правові документи, які визнають право на доступ до інформації основоположним правом людини, а представники організації Об’єднаних націй, Ради Європи, ОБСЄ у своїх доповідях звертають увагу на те, що право на доступ до інформації є необхідною умовою для участі громадян в ухваленні державних рішень, запорукою розвитку демократії та фундаментом у боротьбі з корупцією.

Основними документами, які визначають міжнародні стандарти права на доступ до публічної інформації, на сьогодні є:

1) Конвенція Ради Європи про доступ до офіційних документів від 8.06.2009;

2) Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля (ратифікована Законом України № 832-XIV від 06.07.99 р.);

3) Йоганнесбурзькі принципи. Національна безпека, свобода висловлювань і доступ до інформації;

4) документи міжнародної організації “артикль 19” (Article 19), зокрема: “Право громадськості знати. Принципи законодавства про свободу інформації”, Модельний закон про свободу інформації;

5) “Про доступ до офіційних документів”, рекомендація Rec (2002) 2 Комітету Міністрів Ради Європи від 21.02.2002;

6) “Про доступ до інформації, що перебуває в розпорядженні державних органів”, рекомендація № R (81) 19 Комітету Міністрів Ради Європи від 25.11.1981;

7) “Про доступ громадськості до інформації, що є в розпорядженні державних органів, і свободу інформації”, рекомендація № 854 (1979) Парламентської Асамблеї Ради Європи;

8) “Про право на недоторканість приватного життя”, резолюція № 1165 (1998) Парламентської Асамблеї Ради Європи;

9) практика Європейського суду з прав людини.

Відповідно до перелічених міжнародних документів основними міжнародними стандартами у сфері права на доступ до інформації є:

• принцип максимальної відкритості – уся інформація у володінні публічних органів є відкритою, крім передбачених законом винятків;

• відомості, доступ до яких закривається, мають бути ясними, описуватися вузько і відповідати контролю згідно з “трискладовим тестом”, а саме: 1) інформація повинна мати відношення до легітимної мети, передбаченої законом; 2) оприлюднення інформації повинно загрожувати спричиненням суттєвої шкоди вказаній легітимній меті; 3) шкода, яка може бути заподіяна вказаній меті, має бути вагомішою, ніж суспільний інтерес в отриманні інформації;

• обсяг інформації, доступ до якої обмежується, про публічну особу має бути значно меншим, ніж обсяг інформації про приватну особу;

• процедура доступу до інформації має бути чітко визначеною, а загальний строк надання інформації за запитом – стислим;

• передбачено не лише право на доступ до інформації, якою володіють органи державної влади та місцевого самоврядування, а й до інформації, яка належить приватним організаціям, якщо оголошення цієї інформації зменшить ризик шкоди головним суспільним інтересам;

• наявність спеціальний позасудовий механізм захисту права на доступ до

інформації (інформаційний уповноважений);

• захист “викривачів” (“whistleblowers”).

**Контрольні запитання для самоперевірки**

1. Дайте визначення поняття «джерела інформаційного права», охарактеризуйте форми джерел інформаційного права.

2. Проаналізуйте зовнішні форми інформаційного права: інформаційно-правовий прецедент, інформаційно-правовий договір, інформаційно-правовий акт.

3. Дайте визначення категорії «інформаційне законодавство», його класифікація.

4. Міжнародно-правові стандарти в сфері інформаційного права.

## Тема 3. Поняття і класифікація інформації

### 3.1. Поняття «інформація»

Інформація виступає основним об’єктом інформаційного суспільства. З появою нових інформаційних технологій, основою яких є впровадження засобів обчислювальної техніки, зв’язку, систем телекомунікації, інформація стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, громадських організації та громадян. Від її якості та достовірності, оперативності одержання залежать численні рішення, що приймаються на різних рівнях – від глави держави до громадянина.

Поняття “інформація” використовується в усіх галузях науки, і в правовій, зокрема. Воно набуло багатозначності й інтерпретується залежно від сфери вживання.

В перекладі з латинської мови “інформація” (information) – це роз’яснення, виклад; тобто йдеться про відомості (або їх сукупність), про предмети, явища й процеси навколишнього світу. Сьогодні немає усталеного й вичерпного тлумачення цього терміну.

Поняття інформації неодноразово змінювалось. Вперше термін “інформація” знайшов своє відображення у математичній теорії інформатики і теорії передачі даних каналами зв‘язку Клода Шеннона (1948), в якій він під “інформацією” розумів усі види повідомлень. К. Шеннон разом з У.Уівером запропонували імовірні методи для визначення кількості інформації, що передається. Однак такі методи описують лише знакову структуру інформації, не зачіпаючи її змісту.

Н. Вінер запропонував “інформаційне бачення” кібернетики, як науки про управління в живих організмах та технічних системах. Під інформацією почали розуміти вже не будь-які відомості, а лише ті, які є новими та корисними для прийняття такого рішення, що забезпечить досягнення мети управління. Інші відомості не вважались інформацією.

Розглядаючи інформацію як предмет правовідносин у правовій системі, предмет взаємовідносин між державою та юридичними і фізичними особами, доводиться повертатися до вихідних визначень інформації. Прикладом може стати визначення, яке запропонував С.І. Ожегов. На його думку, інформація - це: 1) відомості про навколишній світ і процеси, що в ньому відбуваються; 2) повідомлення про стан справ, про стан чого-небудь.

Для того, щоб окреслити інформацію у правовому контексті, ми повинні виділити такі юридично значимі ознаки, які зумовлюють специфіку інформації як об’єкта правового регулювання. До таких ознак найчастіше відносять:

- нематеріальний характер (“самостійність відносно носія”, тобто цінність інформації полягає в її суті, а не в матеріальному носії, на якому вона зафіксована);
- суб‘єктивний характер (“інформація виникає в результаті діяльності суб‘єкта, який наділений свідомістю”, тобто вона є результатом інтелектуальної діяльності);
- необхідність об‘єктивації для включення у правовий обіг;
- кількісна визначеність;

- неспоживчість, можливість багаторазового використання;
- зберігання інформації у суб‘єкта, який її передає;
- здатність до відтворення, копіювання, збереження і накопичення.

Отже, інформація – це об’єкт багатофункціональний. Вона створюється й застосовується в усіх сферах діяльності і забезпечує виконання багатоманітних функцій і завдань, що постають перед найрізноманітнішими суб’єктами – органами державної влади, місцевого самоврядування, перед фізичними і юридичними особами, іншими соціальними утвореннями. Саме тому Закон України “Про інформацію” від 02.10.1992 р. розуміє інформацію як “документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

З правової точки зору, інформація виступає об‘єктом інформаційних правовідносин.

Якщо розглядати інформацію в контексті інформаційного суспільства, то вона (інформація) разом із знаннями виступає головним продуктом і основою його функціонування. Функціонування інформаційного суспільства забезпечується розвитком інформаційної інфраструктури, одним з основних елементів якої є інформаційні ресурси. Інформаційні ресурси становлять собою документи та масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах та ін.); тобто, вони виступають джерелами інформації.

Інформаційне суспільство у правовому відношенні функціонує на основі нормативних актів, які регламентують інформаційні відносини й процеси, в тому числі відносини власності на інформаційні ресурси та авторські права, доступ до публічної інформації, захист інформації, права на інтелектуальну власність, використання інформаційних технологій у державному управлінні.

Таким чином, *інформація* виступає об’єктом інформаційних відносин, які пов’язані з реалізацією права на інформацію та інформаційною діяльністю у

галузі створення, збирання, отримання, використання, поширення та зберігання інформації. З точки зору функціонування інформаційного суспільства цікавим є питання саме використання інформації (задоволення інформаційних потреб суб'єктів інформаційних відносин), проблема доступу до неї. Право на доступ до інформації та недоторканості особистості є загальними правами людини, їх законодавче оформлення створює правовий фундамент інформаційного суспільства. Тому, розглянемо дану проблематику.

Функціонування інформаційного суспільства можливе лише за умов існування демократичної, правової держави, де панує принцип верховенства права і максимально забезпечується реалізації прав людини. Право на доступ до інформації є одним з невід'ємних прав людини і громадянина.

*Основними елементами інформаційної сфери є:*

(а) інформація, в тому числі інформаційні ресурси (документи, банки й бази даних, архіви, бібліотеки, музейні фонди тощо);

(б) інформаційна інфраструктура (організаційні структури, що забезпечують збирання, оброблення, зберігання, розповсюдження, пошуки й передачу інформації, а також гарантують інформаційну безпеку; інформаційно-телекомунікаційні структури; інформаційні, комп'ютерні й телекомунікаційні технології; системи засобів масової інформації).

Сукупність відомостей, інформації про що-небудь є інформаційним ресурсом. Інформаційний ресурс створюється людиною; це, як правило, документована інформація, що точніше виражає її функціональне призначення.

При правовому регулюванні інформаційних відносин повинні враховуватися юридичні властивості інформації.

Відповідно до законодавства України *інформація* - це відомості про осіб, предмети, факти, події, явища і процеси, незалежно від форми їх подання.

### 3.2. Класифікація інформації

Інформація класифікується за:

*а) за роллю в правовій системі*:

1) Правова інформація, яка поділяється на:

- нормативну правову інформацію (створюється в порядку правотворчої діяльності та міститься в нормативних правових актах);
- ненормативну правову інформацію (створюється в порядку правозастосовчої та правоохоронної діяльності).

До ненормативної правової інформації можна віднести загальну інформацію про стан законності і правопорядку, інформацію про цивільно-правові відносини, договірні та інші зобов'язання.

2) Неправова інформація.

*б) за ступенем доступності:*

1) Відкрита інформація. До відкритої можна віднести офіційні документи, інформацію про результати виборів, референдумів та ін.

2) Інформація обмеженого доступу. До інформації з обмеженим доступом відносяться конфіденційна, таємна та службова.

Інформація має свої, властиві тільки їй *ознаки*, що мають універсальний характер у будь-яких формах її існування.

1. *Ідеальність і несамостійність* інформації. Поки інформація в пам'яті людини, вона ідеальна, у разі перенесення на матеріальний носій інформація не матеріалізується, вона залишається ідеальною для суб'єктів, які її використовують. Є матеріальним лише носій інформації. Несамостійність інформації проявляється у неможливості для неї існувати і функціонувати без матеріального носія.

2. *Невичерпність* інформації виявляється в тому, що інформація при її передачі може мати необмежену кількість користувачів і при цьому залишатися незмінною.

3. Ознака *наступності* інформації проявляється у тому, що всі зміни інформації супроводжуються змінами в матеріальних системах, що носять поступальних характер і забезпечується спадкоємність станів як на фізичному, так і на інформаційному рівні.

4. *Трансформування* інформації означає можливість передавати один і той же зміст в різній формі і при різних способах пред'явлення.

5. *Універсальність* інформації виявляється в тому, що її зміст може бути пов'язано з будь-якими явищами і процесами фізичної, біологічної, соціальної реальності.

6. *Комплексна якість інформації* характеризує відповідність інформації потребам системи по наступним параметрами: адекватність, вірогідність, повнота, доступність, цінність інформації.

### 3.3. Право на інформацію та її обмеження.

Конституція України закріпила право людини на свободу інформації. Стаття 34 Конституції України гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб і на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобіганню розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Ця норма Конституції України ґрунтується на положеннях Європейської конвенції про захист прав та основних свобод людини, Міжнародного пакту про громадянські і політичні права (стаття 18, 19) та ін.

Це право повинно забезпечуватися, в першу чергу, наявністю відповідного ефективного законодавства, що є правовою підставою забезпечення здійснення конституційного права людини на свободу інформації, а також наявністю реальних механізмів здійснення цього права.

Насправді сьогодні існує багато труднощів у сфері доступу громадян до публічної інформації (інформації, якою володіють органи державної влади та

органи місцевого самоврядування). Свідченням цього є скарги громадян на відмову в задоволенні запитів на інформацію до органів вищого рівня чи суду. Органи державної влади та органи місцевого самоврядування фактично безпідставно відмовляють у наданні інформації, відносячи її до інформації з обмеженим доступом; існують великі труднощі в отриманні громадянами локальних нормативно-правових актів (а в деяких випадках це взагалі неможливо) місцевих органів виконавчої влади та органів місцевого самоврядування.

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом (стаття 20 Закону України "Про інформацію"). Інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову.

*Конфіденційною* є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами. Питання щодо таємної інформації регулюється Законом України "Про державну таємницю" від 21 січня 1994 року.

### 3.4. Моделі здійснення права на інформацію в європейських країнах

Щодо здійснення права на інформацію в європейських країнах, використовують кілька *моделей* при реалізації відповідних положень.

(1) Закон про свободу інформації трактується як нормативний акт, що має силу конституції, і тому він є законом прямої дії для всіх державних інституцій. Це означає, що не існує окремого органу, який виконує положення цього закону

та не існує окремих структур у системі виконавчої влади, які відповідають виключно за питання доступу до публічної інформації. Зазвичай, нагляд за реалізацією закону здійснюють парламенти, а у випадку захисту інтересів громадян – омбудсмени та суди.

(2) В деяких країнах реалізація положень закону законів про свободу інформації супроводжувалась створенням окремих органів, які відповідали за підготовку підзаконних актів та за координацію процесу впровадження відповідних програм у системі державного управління. Подібні органи функціонували від двох до п’яти років та були ліквідовані після виконання покладених на них функцій та завдань. Підготовчий етап запровадження відповідних механізмів у сфері доступу до інформації було віднесено до сфери повноважень Міністра юстиції, або до компетенції Міністра фінансів.

(3) Кілька країн застосовували іншу стратегію для здійснення управління питаннями доступу до інформації – вони прийняли рішення про створення окремих органів виконавчої влади, які будуть відповідати за весь спектр питань, пов’язаних з інформацією.

Загальноприйнятою практикою для більшості європейських країн є розмежування інформаційних служб в організаційній структурі кожного державного органу. Основне завдання цих послуг – сприяти потоку інформації між відповідним державним органом, засобами масової інформації та пересічними громадянами.

Інформаційні служби в сучасних урядах європейських країн відповідають за надання громадянам комплексної та достовірної інформації щодо всіх аспектів діяльності уряду на всіх можливих типах інформаційних носіїв. Комплексний характер цієї діяльності призводить до того, що, зазвичай, інформаційні послуги діляться на дві частини: послуги, які надаються через урядовий інформаційний центр та інформаційні служби в міністерствах.

В основному структурні підрозділи виконують п’ять груп завдань:

- консультативні послуги для службовців, які обіймають посади спеціалістів департаментів;

- організація комунікацій зі ЗМІ;

- надання інформації громадянам;

- дослідження та аналітична робота;

- координація інформаційної політики та покращення інформаційних потоків всередині урядових органів.

Одним з механізмів реалізації права на доступ до інформації є інститут омбудсменів і та роль, яку вони виконують при реалізації права на доступ до інформації.

До сфери повноважень омбудсмена віднесено здійснення нагляду за функціонуванням державних та місцевих органів влади, а також державних інституцій. Більшість омбудсменів наділені правом пропонувати парламенту скасувати, внести зміни до чинного та прийняти нові акти законодавства.

Окрім цього, наприклад, у Великобританії створено Документ про Відкритий уряд, що декларує безкоштовне і безперешкодне одержання інформації, що стосується прав і привілеїв громадян. А спеціальний кодекс регулює практику доступу до урядової інформації, з яким, до речі, можна ознайомитися в Інтернеті.

У Швеції й Австрії всі офіційні документи вважаються суспільно важливими, якщо тільки вони не віднесені законом до секретних. Більш того, в Австрії, якщо виникає попит на секретну інформацію, представники влади вправі вирішувати, чи зберегти конфіденційність чи задовольнити зацікавленість громадськості і розкрити її.

Для вирішення проблем, пов’язаних із забезпеченням доступу до інформації необхідно чітко, на законодавчому рівні, визначити інформацію, доступ до якої обмежується, і мету обмеження.

**Контрольні запитання для самоперевірки**

1. Визначення поняття «інформація».

2. Класифікація інформації, її ознаки.

3. Право на інформацію та її обмеження.

4. Моделі здійснення права на інформацію в європейських країнах

**Тема 4. Інформаційно-правові норми та інформаційно-правові відносини (їх сутність, структура, види).**

**4.1. Зміст і особливості правової норми.**

Правове регулювання в інформаційній сфері забезпечується сукупністю норм різних галузей права – конституційного, адміністративного, цивільного, кримінального та ін.

Правові норми в сфері інформаційного права - це встановлені державою й забезпечені в разі необхідності державним примусом загальнообов'язкові приписи, правила поведінки, які покладаються на учасників суспільних відносин шляхом надання суб’єктам певних прав та покладення обов’язків.

Предметом регулювання правових норм в сфері інформаційного права становлять суспільні відносини в інформаційній сфері. У більшості випадків такі норми мають імперативний характер. Інформаційно-правова норма, як форма діяльності суб’єктів інформаційного права, має класичну структуру. Ці норми поділяють на види за різними критеріями; а реалізуються вони шляхом їх виконання, дотримання, використання або застосування тощо.

Норма права як особливий засіб регулятивного впливу на суспільство характеризується певними ознаками, які надають цій категорії самостійного значення та відрізняють від інших засобів соціального впливу.

1. Правова норма пов'язана з державою. Вона являє собою владний припис, що встановлюється чи санкціонується державою та відображає її волю.

2. Норма права має владний характер. Вона визначає важливі державі та суспільству відносини і регулює їх.

3. Це правило поведінки, що визначає модель можливої та необхідної поведінки суб'єктів, яка відповідає інтересам суспільства та держави. Завдяки

нормі суб'єкти можуть визначити правомірність чи протиправність своєї поведінки. Зміст норми складають права як можливість вчиняти правомірні дії для реалізації власних інтересів; обов'язки як необхідність виконання необхідної поведінки та заборони як необхідність утриматися від вчинення дій певного роду.

4. Це загальнообов'язкове правило поведінки, що має загальний характер, поширюючись на невизначену кількість випадків та невстановлене число суб'єктів. Правова норма є правилом поведінки кожного суб'єкта, який перебуває у сфері правового регулювання

5. Формальна визначеність норми виявляється у її зовнішньому прояві шляхом закріплення у тексті певного правового документа. Формальна визначеність норми повною мірою забезпечує її юридичний характер.

6. Має визначену структуру - складається із взаємопов'язаних елементів: гіпотези, диспозиції, санкції; разом з іншими нормами утворює систему права;

7. Гарантованість державою означає можливість створення системи гарантій реалізації норми, забезпечення необхідних умов для добровільного виконання приписів суб'єктами, а також застосування державного примусу до суб'єктів, які порушують нормативні установлення.

8. Логічність норми виявляється у встановленні нею логічно завершеної моделі поведінки суб'єктів та наявності логічного змісту і структури. Форму логічності норми права можливо визначити тезами:

— якщо суб'єкт права діє в ситуації, що регулюється правом, він повинен вчиняти поведінку, яка вимагається;

— якщо суб'єкт не вчиняє поведінку, що вимагається нормою права, він має нести відповідальність.

### 4.2. Класифікація інформаційно-правових норм.

Інформаційно-правові норми *за методом правового регулювання* (або за формою закріплення бажаної поведінки суб'єктів права): імперативні, диспозитивні.

**Імперативні** — норми, що виражають у категоричних розпорядженнях держави чітко позначені дії і не допускають ніяких відхилень від вичерпного переліку прав і обов'язків суб'єктів. Інакше: імперативні норми прямо наказують правила поведінки.

**Диспозитивні** — норми, у яких держава наказує варіант поведінки, але які дозволяють сторонам регульованих відносин самим визначати права й обов'язки в окремих випадках, їх називають «заповнювальними», оскільки вони заповнюють відсутність угоди і діють лише тоді, коли сторони регульованих відносин не встановили для себе іншого правила, не домовилися з даному питання (розпізнаються через формулювання: «за відсутності іншої угоди», «якщо інше не встановлено в договорі» та ін.). Інакше: диспозитивні норми надають свободу вибору поведінки.

Інформаційно-правові норми *за характером впливу на особу*: заохочувальні, рекомендаційні. **Заохочувальні** — норми, що встановлюють заходи заохочення за варіант поведінки суб'єктів, який схвалюється державою і суспільством і полягає в сумлінній і продуктивній праці (наприклад, правила щодо виплати премій). **Рекомендаційні** — норми, що встановлюють варіанти бажаної з погляду держави поведінки суб'єктів.

Інформаційно-правові норми *по субординації в правовому регулюванні*: матеріальні, процесуальні. **Норма матеріального права** — норма, що є первинним регулятором суспільних відносин: містить правило (права, обов'язки, заборони), на підставі якого можливо вирішення справи по суті. Наприклад, не можна вчиняти вбивство. **Норма процесуального права** — норма, що встановлює оптимальний порядок застосування норм матеріального права: містить правило, на підставі якого можливо вирішення справи по суті.

Наприклад, порядок розслідування злочину, порядок виклику свідків до суду тощо.

Інформаційно-правові норми *за ступенем визначності варіанта поведінки*: абсолютно визначені, відносно визначені. **Абсолютно визначені норми права -** це норми з вичерпною конкретністю і повнотою встановлюють умови своєї дії, права і обов'язки адресатів та наслідки їх порушення. **Відносно визначені норми права** — це норми, що не містять повних, вичерпних вказівок на умови їх дії, права та обов'язки адресатів або зміст санкцій.

### 4.3. Структура інформаційно-правової норми.

Структура норми залежить від її характеру. До визначення структури можна підійти по-різному, залежно від того, яка це норма — норма-принцип, норма-дефініція, норма-правило поведінки.

Нормами, що містять безпосередні правила поведінки для конкретних (але не індивідуалізованих) суб'єктів в реальному суспільному житті є: норми-дозволу; норми-приписи (зобов'язування); норми-заборони.

Для позначення структурних елементів норми права теорія права оперує такими поняттями: **диспозиція**, **гіпотеза**, **санкція**.

***Диспозиція*** — центральний елемент норми права, в якому у вигляді владного припису закріплено правило поведінки, змістом якого виступають суб'єктивні права та юридичні обов'язки. Види диспозицій:

1. За ступенем визначеності:

- *Визначені* — закріплюють однозначне правило поведінки, тобто учасники відносин позбавлені можливості для вибору іншої поведінки;
- *Не повністю визначені* — вказують лише на загальні ознаки поведінки, в рамках яких суб'єкти уточнюють свої права та обов'язки самостійно;
- *Відносно визначені* — вказують на права і обов'язки суб'єктів, але надають можливості для їх уточнення залежно від конкретних обставин;
- *Альтернативні* — вказують на настання декількох правових наслідків, але передбачають настання лише одного з них.

2. За способом викладення:

- *Проста* — правило поведінки визначається у загальному вигляді без деталізації його ознак;
- *Описова* — правило поведінки закріплюється повно, з деталізацією його ознак; чітко визначаються права і обов'язки учасників відносин;
- *Бланкетна* — закріплюється лише загальні ознаки правила поведінки, а для встановлення ознак, яких бракує, слід звертатися до норм іншого нормативного акта іншої галузі права;
- *Відсильна* — аналогічна бланкетній з тією різницею, що для встановлення ознак, яких бракує, слід звертатися до інших частин даної норми або до інших норм цієї ж галузі права.

3. За складом:

- *Прості* — містять одне правило поведінки;
- *Складні* — містять два або більше обов'язкових правил поведінки;
- *Альтернативні* — містять декілька правил поведінки, суб'єкт може виконувати будь-яке з них.

***Гіпотеза*** — структурний елемент норми права, який вказує на умови, за наявності або відсутності яких вступає в дію правило поведінки. Гіпотеза — невід'ємний елемент норми; її точність і визначеність є умовою реалізації норми. Відсутність такої визначеності ускладнює використання передбачених нормою можливостей її адресатами — громадянами, та їх об'єднаннями. Якщо ж норма закріплює повноваження державного органу, то невизначеність перерахованих в її гіпотезі умов надає йому право діяти на власний розсуд. Види гіпотез:

1. За ступенем визначеності:

- *Визначена* — вичерпно визначає ті умови, при наявності яких набуває чинності правило поведінки, що міститься у диспозиції норми права;
- *Відносно визначена* — обмежує умови застосування норми права певним колом формальних ознак.

2. За формою вираження:

- *Абстрактні* — умови застосування норми визначаються загальними родовими ознаками, що надає можливість охопити та врегулювати значну кількість однорідних випадків;
- *Казуальні* — визначаються умови дії норми, використовуючи більш вузькі, спеціальні родові ознаки, тому норма права поширюється на обмеженіше коло випадків.

3. За складом:

- *Прості* — містять одну обставину, необхідну для дії правової норми;
- *Складні* — містять дві або більше обов'язкових обставин, за якими пов'язується дія правової норми;
- *Альтернативні* — чинність норми права визначається залежно від однієї або кількох фактичних обставин (умов) і для настання правових наслідків досить наявності однієї з цих обставин.

***Санкція*** — це частина норми права, яка містить вказівки щодо юридичних наслідків порушення правила, зафіксованого в диспозиції. Мета санкції — створення тих чи інших несприятливих наслідків для правопорушника або заохочувальних наслідків для суб'єктів, що виконують владний припис.

Види санкцій:

1. За ступенем визначеності:

- *Абсолютно визначені* — чітко визначають вид та міру юридичної відповідальності;
- *Відносно визначені* — межі юридичної відповідальності визначаються від мінімальної до максимальної або тільки до максимальної;

2. За кількістю несприятливих наслідків:

- *Прості* - передбачають один невигідний наслідок.
- *Складні*-передбачають одночасне застосування декількох невигідних наслідків.

• *Альтернативні* — вказують на декілька можливих засобів впливу на правопорушника, а доцільність застосування конкретного засобу визначається правозастосовчим органом, виходячи з особливості конкретної справи;

3. За характером наслідків:

• *каральні (штрафні); правовідновлювальні (компенсаційні); заохочувальні.*

4. За галузями права:

• *кримінально-правові; адміністративно-правові; цивільно-правові.*

Від класичної (трьохелементної) норми слід відрізняти *нормативно-правовий припис* - цілісне, логічно і граматично завершене судження загального характеру, що формально закріплене в тексті нормативно-правового акту чи іншого джерела права. Як первинний елемент нормативно-правового акту, нормативно-правовий припис має зазвичай форму статті чи пункту цього акту. Його структура є двохелементною: у зобов'язальних приписах - гіпотеза-диспозиція (якщо - то); в заборонних приписах - диспозиція-санкція (то -а інакше).

Нормативний припис виступає техніко-юридичним способом функціонування норми права, яку правозастосувач має встановити у повноті її елементів (у структурній єдності гіпотези, диспозиції, санкції) шляхом логічного аналізу, інтелектуальної роботи, тлумачення. Так, у нормативних приписах кримінального закону гіпотези є передбачуваними, гіпотетичними, які встановлюються шляхом тлумачення.

Нормативно-правові приписи, що містяться в нормативно-правових актах та інших джерелах права, за характером регулювання суспільних відносин можна поділити на приписи прямого регулювання (правила поведінки) і приписи опосередкованого регулювання (спеціалізовані приписи - установчі, дефінітивні, декларативні, прогностичні, оперативні тощо).

**Контрольні запитання для самоперевірки**

1. Зміст і особливості правової норми.

2. Класифікація інформаційно-правових норм.

3. Структура інформаційно-правової норми.

## Тема 5. Поняття, ознаки та види інформаційних правовідносин

### 5.1 Поняття та ознаки інформаційних правовідносин.

Інформаційні правовідносини розуміються як урегульовані правовими нормами суспільні відносини, які виникають з приводу інформації, сторони якого виступають як носії взаємних прав та обов’язків, установлених і гарантованих інформаційно-правовою нормою.

Інформаційні правовідносини виникають саме в рамках інформаційної сфери. Такі відносини неоднорідні і включають в себе декілька груп суспільних відносин, що виникають в інформаційній сфері з приводу інформації:

1. відносини, пов'язані зі створенням і перетворенням інформації (створення офіційної інформації);

2. відносини, пов'язані зі зберіганням інформації (захист інформації, зберігання інформації з особливим режимом доступу);

3. відносини, пов'язані з передачею та розповсюдженням інформації (правове становище засобів масової інформації, поширення інформації за допомогою використання мережі Інтернет тощо глобальних інформаційних мереж);

4. відносини, пов'язані зі споживанням інформації (реалізації прав громадян на інформацію, відносини у сфері бібліотечної та архівної справи).

Можна виділити наступні ознаки інформаційних правовідносин:

- наявність конкретного основного чи другорядного об'єкту відносин - інформації;
- відносна соціальна значимість інформації – об'єкту відносин (суспільно значима інформація, національно значима, особиста чи економічна значимість інформації тощо);

- первинність інформаційно-правової норми, що регулює конкретні суспільні відносини;
- передбачена правовими актами форма правомірної поведінки суб'єктів відносин щодо конкретної інформації;
- наявність взаємних прав та обов'язків суб'єктів-учасників правовідносин, а також юридичної відповідальності за поведінку, що суперечить правовій нормі;
- інші ознаки, що характерні для правовідносин в цілому.

Суспільні відносини щодо інформації, які не відповідають змісту вищезазначених ознак, не можна вважати правовідносинами: відносини між людьми на побутовому рівні щодо надання певної усної інформації, листування через електронну пошту тощо.

Отже, інформаційні правовідносини – це соціальні відносини, врегульовані нормами різних галузей права, що виникають в усіх сферах життєдіяльності людей у процесі обігу (збирання, зберігання, використання і поширення) певної інформації що мас відповідну суспільну значимість.

Збирання інформації – це набуття, придбання, накопичення документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою.

Зберігання інформації – це забезпечення належного стану інформації та її матеріальних носіїв.

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави.

Поширення інформації – це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації.

### 5.2. Елементи інформаційних правовідносин

***Елементи*** інформаційних правовідносин:

- *суб'єкти*, що вступають у правовідносини при здійсненні інформаційних процесів;
- *об'єкти*, у зв'язку з якими суб'єкти вступають у інформаційні правовідносини;
- *права, обов'язки та відповідальність суб'єктів* правовідносин при здійсненні інформаційних процесів (зміст).

**Суб'єкти інформаційних правовідносин** - це суб'єкти інформаційного права, під якими розуміються фізичні та юридичні особи, які є носіями передбачених інформаційним законодавством прав та обов'язків.

Відповідно до ст. 4 Закону України «Про інформацію» суб'єктами інформаційних відносин є: фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень.

**Залежно від місця й ролі в системі інформаційних відносин** суб'єкти інформаційного права поділяються: (а) на органи, що формують політику в інформаційній сфері; (б) на державні органи, на яких покладено безпосередній обов'язок реалізації цієї політики; (в) на інші органи, що здійснюють інформаційну діяльність.

Однак для того, щоб виступати в ролі суб'єкта інформаційних правовідносин, необхідно мати інформаційну правоздатність та інформаційну дієздатність.

Під *інформаційною правоздатністю* розуміється визнана правовими нормами фактична можливість або здатність суб'єкта мати суб'єктивні інформаційні права і виконувати суб'єктивні інформаційні обов'язки. У той же час здатність володіти суб'єктивними інформаційними правами і обов'язками не означає здатності самостійно їх набувати і здійснювати. У даному випадку необхідна *інформаційна дієздатність,* під якою розуміється здатність і можливість суб'єкта своїми діями набувати суб'єктивні юридичні права, створювати для себе юридичні обов'язки, а також нести відповідальність за свої дії в інформаційній сфері.

Залежно від обсягу інформаційних прав та обов’язків виокремлюють і загальні та спеціальні суб’єкти. Загальними суб’єктами інформаційно-правових відносин є держава, фізичні і юридичні особи будь-якої форми власності. Спеціальні суб’єкти інформаційно-правових відносин це державні службовці, військовослужбовці, посадові та інші особи.

Основним **об’єктом інформаційно-правових відносин** служить інформація, яку Закон України “Про інформацію” визначає як документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі й у навколишньому природному середовищі.

Об’єктом правового регулювання є не тільки інформація, а й інформаційні ресурси, інформаційні системи, технології й засоби їх забезпечення.

Коваленко Л.П. об’єктом інформаційного права слід вважає сукупність однорідних суспільних відносин, реалізація яких здійснюється в межах інформаційної діяльності або інформаційно-правового захисту і потребує відповідної нормативно-правової регламентації, яку становить система законодавчих актів, що впорядковують суспільні відносини матеріального і процесуального характеру, в яких реалізуються права, свободи й обов’язки учасників інформаційної діяльності й інформаційно-правового захисту.

**Змістом інформаційних правовідносин** є взаємні права та обов'язки учасників інформаційних правовідносин.

До прав відносяться:

- правомочність на власні дії, що полягає в можливості здійснення фактичних і юридично значущих дій;
- правомочності на чужі дії, які полягають у можливості вимагати від зобов'язаної особи виконання покладених на нього обов'язків;
- правомочність на захист, полягає в можливості вдатися до державно-примусовим заходам у випадку порушення суб'єктивного права або невиконання одним з учасників правовідносини своїх обов'язків.

Обов'язки:

- необхідність здійснювати певні дії або утриматися від них;
- необхідність виконати вимоги уповноваженої суб'єкта;
- необхідність віднести відповідальність за порушення суб'єктивних прав інших учасників правовідносини або за невиконання їх законних вимог.

Інформація розглядається як об’єкт інформаційно-правових відносин.

**5.3. Види інформаційних правовідносин.**

Розглянемо основні види інформаційних правовідносин. У навчальній літературі відсутня єдина точка зору щодо їх класифікації. Так, Б.А. Копилов виділяє відносини, що виникають:

- при здійсненні пошуку, отримання та споживання інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг;
- при виробництві, передачі та розповсюдженні інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг;
- при створенні та застосуванні інформаційних систем, їх мереж, засобів забезпечення;
- при створенні та застосуванні засобів та механізмів інформаційної безпеки.

Ряд авторів поділяє інформаційні правовідносини на безпосередньо інформаційні правовідносини та відносно-визначені інформаційні правовідносини.

Під *безпосередньо інформаційними правовідносинами* треба розуміти відносини, що виникають з приводу створення інформації, визначення прав власності на неї (з наданням права володіння, користування та розпорядження), а також її обігу (передачі іншим суб'єктам, обробки, аналізу, переробки, споживання) та захисту. В таких правовідносинах інформація виступає основним самостійним об'єктом незалежно від форми (документ, відеозапис, книга, сценарій, лазерний диск із записом тощо). В переважній більшості випадків такі відносини мають охоронюваний характер, націлений на

попередження дій, що порушують чи посягають на інформаційні права суб'єктів. Серед них також є відносини регулятивного характеру, які встановлюють статуси суб'єктів, закріплюють їх права в сфері набуття та реалізації інформаційних прав.

*Відносно-визначені інформаційні правовідносини* – це частина інших правових відносин (цивільних, адміністративних тощо), умовно відокремлених від однорідних, які реалізуються з приводу неінформаційних об'єктів, що впливає на обіг певної інформації. В таких відносинах інформація є факультативним (додатковим) об'єктом правовідносин, що існує паралельно з основним неінформаційним об'єктом. Наприклад, відносини в сфері адвокатської, аудиторської діяльності тощо.

Інформаційні правовідносини класифікують:

1. **регулятивні та охоронні**.

*Регулятивні* правовідносини пов'язані з вольовою діяльністю з пошуку, накопичення, передачі, виробництва та розповсюдження інформації, наприклад доступ фізичних та юридичних осіб до державних інформаційних ресурсів.

*Охоронні* правовідносини виникають у зв'язку з вчиненням правопорушення. Дане правовідношення має місце, коли виникають незаконні обмеження прав засобів масової інформації;

2. **матеріальні і процесуальні**.

*Матеріальні* - складаються з приводу реалізації прав і обов'язків суб'єктів цих відносин, наприклад, у результаті реалізації права громадянина або організації на спростування не відповідають дійсності і ганьблять їх честь і гідність відомостей.

*Процесуальні* - складаються з приводу процедури їх виникнення, зміни, припинення, наприклад при оформленні громадян на допуск до відомостей особливої важливості, цілком таємним і секретних відомостей;

Єдиної точки зору на характер правовідносин, що регулюють інформаційне законодавство, в теорії інформаційного права немає. Більшість

дослідників (В.А. Копилов та ін.) вважають, що інформаційне законодавство регулює виключно відносини, безпосередньо пов'язані з обігом інформації, що виникають в інформаційній сфері у зв'язку з реалізацією інформаційних прав та свобод, здійсненням інформаційних процесів при обігу інформації.

А деякі автори (Г. Красноступ) до переліку відносин, які є предметом регулювання джерел інформаційного законодавства, відносять і такі, що пов'язані з електронним зв'язком; передачею даних; технічними засобами радіомовлення та телебачення; спеціальними телекомунікаційними системами; космічними та іншими видами зв'язку; тарифами, зборами, пільгами за послуги зв'язку; засобами масової інформації; реалізацією інформаційної політики України; інформаційною діяльністю та її видами; ліцензуванням інформаційної діяльності; захистом інформації; правом власності на інформацію та відповідальністю за порушення інформаційного законодавства.

При аналітичному огляді навчально-методичної літератури студентам та слухачам *треба віддавати пріоритет першій точці зору,* оскільки не завжди відносини в телекомунікаційній, технічній та інших сферах пов'язані з обігом інформації. В тім, треба зважати на особливість інформаційних відносин, яка полягає в тому, що вони регулюються нормами окремих галузей законодавства в залежності від характеру інформації та інформаційної середи (законодавством про ЗМІ, цивільним законодавством тощо).

Стаття 5 Закону України „Про інформацію" визначає основні принципи інформаційних відносин – вихідні начала, на яких будуються інформаційні процеси в суспільстві: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації.

**Контрольні запитання для самоперевірки**

1. Поняття, ознаки та види інформаційних правовідносин.
2. Визначить та охарактеризуйте елементи інформаційних правовідносин.

3. Дайте визначення поняття «суб'єкти інформаційних правовідносин».

4. Класифікація інформаційно-правових відносин.

## Тема 6. Види юридичної відповідальності в сфері інформаційного права

Законом України «Про інформацію» у ст. 27 визначено, що порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із Законами України.

Статтею 24 Закону України «Про доступ до публічної інформації» зазначено, що відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень:

1) ненадання відповіді на запит;

2) ненадання інформації на запит;

3) безпідставна відмова у задоволенні запиту на інформацію;

4) неоприлюднення інформації відповідно до статті 15 цього закону;

5) надання або оприлюднення недостовірної, неточної або неповної інформації;

6) несвоєчасне надання інформації;

7) необґрунтоване віднесення інформації до інформації з обмеженим доступом;

8) нездійснення реєстрації документів;

9) навмисне приховування або знищення інформації чи документів.

Особи, на думку яких їхні права та законні інтереси порушені розпорядниками інформації, мають право на відшкодування матеріальної та моральної шкоди в порядку, визначеному законом.

Правові норми з приводу відповідальності за порушення законодавства про інформацію містяться в спеціальних кодифікованих актах про певний вид юридичної відповідальності (Кодекс про адміністративні правопорушення, кримінальний кодекс), які описують підстави притягнення до відповідальності й звільнення від неї, відповідну процедуру, санкції та ін. Це не означає, що стаття 24 Закону не має самостійного значення – наведені в частині першій цієї

статті порушення є підставою для притягнення до дисциплінарної відповідальності, наприклад, державних службовців (особливо за підпунктами 1, 4, 7-9 частини першої цієї статті закону).

Відповідальність фізичних осіб, що порушили законодавство про доступ до інформації, може бути таких видів:

- адміністративна – відповідно до статті 212-3 Кодексу про адміністративні правопорушення, якою передбачені штрафи від 25 до 50 неоподатковуваних мінімумів доходів громадян (на 2014 р. на рівні 50% податкової соціальної пільги – 609 грн. , відповідно 15225 – 30450 грн.); за повторне порушення цієї статті – від 50 до 80 неоподатковуваних мінімумів доходів громадян (на 2014 р. – 30450 – 48720 грн.);
- дисциплінарна – оскільки виконання законодавства про доступ до інформації є частиною службових обов'язків багатьох працівників, то вчинення одного з порушень, передбачених у ч. 1 ст. 24 Закону, являє собою дисциплінарний проступок, за який настає дисциплінарна відповідальність. Загальними видами дисциплінарних стягнень є догана і звільнення (ст. 147 Кодексу законів про працю). Але в окремих видах розпорядників інформації законодавством можуть бути встановлені додаткові види санкцій. Наприклад, для державних службовців такими є попередження про неповну службову відповідність та затримка до одного року в присвоєнні чергового рангу або у призначенні на вищу посаду (ст. 14 Закону «Про державну службу»).

В рамках трудового права існує також матеріальна відповідальність, яка може бути накладена на працівників, що порушенням свої трудових обов'язків заподіяли шкоду роботодавцю. Матеріальна відповідальність працівника може наставати, якщо його роботодавця з вини цього працівника було притягнуто до цивільно-правової відповідальності, що виразилась у стягненні з роботодавця-розпорядника певної суми коштів (детальніше про матеріальну відповідальність див. ст.ст. 130, 132 – 135-1, 135-3 – 138 Кодексу законів про працю);

- цивільно-правова – настає, коли фізична особа безпосередньо є розпорядником інформації (суб'єкт господарювання – розпорядник публічної інформації відповідно до ст. 13 Закону), а також в порядку регресу в окремих випадках існування трудових відносин або коли особа припинила трудові відносини з роботодавцем-розпорядником, працюючи на якого колись завдала майнової шкоди третьому суб'єкту при виконанні трудових обов'язків.

- кримінальна відповідальність за порушення Закону прямо не передбачена, оскільки рівень суспільної небезпеки такого правопорушення не є достатнім для кримінального покарання. Водночас Кримінальний кодекс передбачає відповідальність за окремі випадки порушення права на інформацію, коли це пов'язано із загрозою життю чи здоров'ю людей. Наприклад, за статтею 238 Кримінального кодексу України відповідальність настає за приховування або перекручення відомостей про екологічний стан, що негативно впливає на здоров'я людей, або захворюваність населення в районах з підвищеною екологічною небезпекою. Тому рівень суспільної небезпеки від цього порушення настільки високий, що воно становить склад злочину.

Виною є певне психічне ставлення особи до вчинюваної нею дії чи бездіяльності та її наслідків. Вина може мати форми умислу або необережності. Умисел буває прямий (якщо особа усвідомлювала суспільно небезпечний характер своєї дії або бездіяльності, передбачала її суспільно небезпечні наслідки і бажала їх настання – ст. 24 Кримінального кодексу) і непрямий (якщо особа усвідомлювала суспільно небезпечний характер своєї дії або бездіяльності, передбачала її суспільно небезпечні наслідки і хоча не бажала, але свідомо припускала їх настання – там же). Необережність має місце, коли особа не передбачала можливості настання суспільно небезпечних наслідків своєї дії або бездіяльності, хоча повинна була і могла їх передбачити, або коли вона передбачала можливість настання суспільно небезпечних наслідків своєї дії або бездіяльності, але легковажно розраховувала на їх відвернення (ст. 25 Кримінального кодексу).

Частина друга статті 24 Закону України «Про доступ до публічної інформації» закріплює право на компенсацію матеріальної (майнової) та моральної (немайнової) шкоди шляхом притягнення розпорядника інформації до цивільно-правової відповідальності “в порядку, визначеному законом”. Таким порядком є судове провадження, яке може здійснюватися за процедурами:

• адміністративного судочинства – відповідно до Кодексу адміністративного судочинства, якщо вимогу про відшкодування шкоди, заподіяної протиправними рішеннями, діями чи бездіяльністю суб’єкта владних повноважень заявлено в одному провадженні з вимогою вирішити публічно-правовий спір (ч. 2 ст. 21 КАС);

• цивільного судочинства – згідно із Цивільним процесуальним кодексом (цивільний позов);

• господарського судочинства – згідно з Господарським процесуальним кодексом (позов у господарському процесі; застосовується, лише якщо і потерпілий, і розпорядник є юридичними особами або розпорядник є фізичною особою – підприємцем, а потерпілий – юридичною особою).

Незважаючи на різні види судового провадження, стягнення з розпорядника компенсації за шкоду є проявом цивільно-правової відповідальності, оскільки саме їй притаманний компенсаційний і майновий характер. Така відповідальність спрямована, насамперед, на поновлення порушеного права, а не покарання порушника, як у випадку з дисциплінарною, адміністративною чи кримінальною відповідальністю.

Визначимо риси правопорушень в сфері інформаційного права, а саме: (а) наявність підстави для вчинення правопорушення в даній сфері, а відповідальність за правопорушення настає, якщо відповідно до закону воно за своїм характером не тягне за собою кримінальної чи іншої юридичної відповідальності; (б) правопорушення у даній сфері повинні розглядатися в

позасудовому порядку; (в) відповідальності підлягають як фізичні, так і юридичні особи.

*Інформаційне правопорушення* (проступок) це протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на врегульовані законами суспільні відносини, які виникають та існують при здійсненні діяльності в сфері інформаційного права, а саме: при одержанні, використанні, поширенні та зберіганні учасниками інформаційних правовідносин інформації і за яку законом передбачено відповідальність.

Ознаки правопорушення в сфері інформаційного права:

- **діяння** - лише усвідомлювані особою акти поведінки, виражені як у діях, так і в бездіяльності, можуть вважатися правопорушенням. Як приклади дій, що є правопорушеннями у зазначеній сфері: ненадання інформації на запит, нездійснення реєстрації документів, необґрунтоване віднесення інформації до інформації з обмеженим доступом ст. 24 Закону України «Про доступ до публічної інформації».
- **протиправність -** правопорушення полягає в порушенні правил поведінки, встановлених відповідними правовими нормами.

Склад правопорушення містить чотири необхідні елементи: об'єкт, об'єктивну сторону, суб'єкта і суб'єктивну сторону правопорушення.

**Об'єкт правопорушення** — це ті суспільні відносини та цінності, що охороняються правом, на які спрямовано посягання суб'єктів правопорушення (наприклад, інформація, інформаційні мережі та ін.).

Види об’єктів:

*загальний* - усі суспільні відносини, врегульовані нормами інформаційного права. Виходячи з визначення інформаційного правопорушення загальним об’єктом інформаційного правопорушення є суспільні відносини у інформаційній сфері;

*родовий* - група однорідних суспільних відносин, урегульованих нормами інформаційного права;

*безпосередній* - конкретні суспільні відносини, врегульовані нормами інформаційного права.

*Об'єктивна сторона* інформаційного правопорушення це зовнішні ознаки та обставини, які характеризують правопорушення в сфері інформаційного права.

Ознаки об'єктивної сторони інформаційного правопорушення

1. Обов'язкові:

а) діяння дія чи бездіяльність;

б) шкідливі наслідки негативні зміни, що мають місце в результаті вчинення правопорушення.

Виходячи з наявності чи відсутності матеріальних шкідливих наслідків розрізняють два види правопорушень у зданій сфері: з матеріальним складом і з формальним складом.

До першого виду відносять такі, для яких обов'язковим елементом є настання матеріальних шкідливих наслідків.

До другого виду відносять правопорушення, для яких факт настання матеріальних шкідливих наслідків не є обов'язковим; для них сам факт учинення правопорушення свідчить про настання шкідливих наслідків;

в) причинний зв'язок між діянням і шкідливими наслідками. Насамперед стосується до правопорушень із матеріальним складом, де необхідно чітко встановити, що діяння передувало настанню шкідливих наслідків і між ними є причинний зв'язок.

2. Необов'язкові (факультативні):

а) місце вчинення правопорушення;

б) час учинення правопорушення;

в) засоби вчинення правопорушення;

г) обставини вчинення правопорушення.

Суб'єкт адміністративного правопорушення це особа, яка вчинила інформаційне правопорушення. Суб'єктом адміністративного правопорушення

може бути фізична особа яка досягла 16-річного віку, та юридична особа незалежно від форми власності. Види суб'єктів адміністративного правопорушення: загальні; спеціальні.

Суб'єктивна сторона адміністративного правопорушення - внутрішнє психічне ставлення суб'єкта правопорушення до скоєного діяння та його шкідливих наслідків.

Ознаки суб'єктивної сторони:

1. *Вина* - психічне ставлення особи до скоєного діяння та його шкідливих наслідків. Це обов'язкова ознака суб'єктивної сторони, що проявляється у формі умислу чи необережності.

Умисел має місце у правопорушенні тоді, коли особа, яка його вчинила, усвідомлювала протиправний характер своєї дії чи бездіяльності, передбачала її шкідливі наслідки і бажала їх або свідомо допускала настання цих наслідків.

Необережність має місце у правопорушенні тоді, коли особа, яка його вчинила, передбачала можливість настання шкідливих наслідків своєї дії чи бездіяльності, але легковажно розраховувала на їх відвернення або не передбачала можливості настання таких наслідків, хоча повинна була і могла їх передбачити.

Мотив це усвідомлювана причина, яка спонукає особу до скоєння правопорушення

2. *Мета* це очікуваний результат, бажані наслідки, яких прагне досягти особа вчиненням правопорушення.

Керуючись необхідністю визначення чітких відмінностей між правопорушеннями в сфері інформаційного права, адміністративними, дисциплінарними правопорушеннями та злочинами, наведімо основні ознаки, що характеризують вказані відмінності: законодавство, орган юрисдикції, ступінь суспільної небезпеки, юридичні наслідки притягнення до відповідальності.

Органом юрисдикції за злочин є виключно суд, а за правопорушення в сфері інформаційного права крім адміністративного суду, інші органи адміністративної юрисдикції, суди тощо. Одним із елементів поняття відповідальності за правопорушення в сфері інформаційного права є санкція за невиконання припису правової норми.

У Кримінальному кодексі України до злочинів в інформаційній сфері можна віднести більше 50 статей, на жаль, усі вони містяться у різних розділах КК України, наприклад, у розділі УП «Злочини у сфері господарської діяльності» є 4 статті щодо злочинів в інформаційній сфері. Наприклад, ст. 231 «Незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю», ст. 232 «Розголошення комерційної або банківської таємниці», ст. 232-1 «Незаконне використання інсайдерської інформації», ст. 232-2 «Приховування інформації про діяльність емітента». Також ст. 182 КК України передбачає кримінальну відповідальність за порушення недоторканності приватного життя, зокрема за збирання, зберігання, використання або поширення інформації про особу без її згоди.

КУпАП передбачає адміністративну відповідальність за правопорушення в інформаційній сфер: ненадання інформації, порушення у порядку її надання, надання неповної інформації та ін. За вчинення адміністративних правопорушень застосовується вид адміністративного стягнення - штраф.

Адміністративним правопорушенням (проступком) визнається протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на громадський порядок, власність, права і свободи громадян, на встановлений порядок управління і за яку законом передбачено адміністративну відповідальність.

До таких правопорушень КУпАП відносить: ст. 41-3 ненадання інформації для ведення колективних переговорів та здійснення контролю за виконанням колективних переговорів, угод; ст. 46 навмисне приховування джерела зараження венеричною хворобою; ст. 53-2 перекручення або

приховування даних державного земельного кадастру; ст. 57 порушення вимог щодо охорони надр; ст. 58 порушення правил та вимог проведення робіт щодо геологічного вивченню надр; ст. 59-1 порушення вимог щодо охорони територіальних та внутрішніх морських вод від забруднення та засмічення; ст. 60 порушення правил водокористування; ст. 62 невиконання обов'язків по реєстрації в суднових документах операцій з шкідливими речовинами та сумішами; ст. 82-1 порушення правил ведення первинного обліку та здійснення контролю за операціями поводження з відходами або неподання чи подання звітності щодо утворення, використання, знешкодження та знищення відходів; ст. 82-3 приховування, перекручення або відмова від надання повної та достовірної інформації за запитами посадових осіб і зверненнями громадян та їх об'єднань щодо безпеки утворення відходів та поводження з ними; ст. 83-1 порушення законодавства про захист рослин; ст. 91-4 відмова від надання чи несвоєчасне надання екологічної інформації; ст. 92-1 порушення законодавства про Національний архівний фонд та архівні установи; ст. 96 недодержання державних стандартів, норм та правил при проектуванні та будівництві; ст. 96-1 порушення законодавства під час планування і забудови територій; ст. 116-3 порушення правил реєстрації торгівельних суден; ст. 148-5 порушення правил про взаємоз'єднання телекомунікаційних мереж загального користування; ст. 156-1 порушення законодавства про захист прав споживачів; ст. 163-1 порушення порядку ведення податкового обліку, надання аудиторських висновків; ст. 164-1 порушення порядку подання декларації про доходи та ведення обліку доходів і витрат; ст. 164-2 порушення законодавства з фінансових питань; ст. 164-6 демонстрування і розповсюдження фільмів без державного посвідчення на право розповсюдження та демонстрування фільмів; ст. 164-9 незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних; ст. 164-14 порушення законодавства про здійснення закупівлі товарів, робіт і послуг за державні кошти; ст. 165-1 порушення законодавства про збір та облік єдиного внеску на

загальнообов'язкове державне соціальне страхування і загальнообов'язкове державне пенсійне страхування; ст. 165-4 порушення законодавства про загальнообов’язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності; ст. 165-5 порушення законодавства про загальнообов'язкове державне соціальне страхування у зв'язку з тимчасовою втратою працездатності та витратами, зумовленими похованням; ст. 166-4 порушення порядку надання інформації та виконання рішень Антимонопольного комітету України та його територіальних відділень та ін.

**Контрольні запитання для самоперевірки**

1. Дайте визначення поняття «інформаційне правопорушення».
2. Які ознаки інформаційного правопорушення.
3. Види юридичної відповідальності в сфері інформаційного права.

**Література до розділу І**

Конституція України / Закон від 28.06.1996 № 254к/96-ВР [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

Кримінальний кодекс України / Закон від 05.04.2001 № 2341-III [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/2341-14.

Цивільний кодекс України / Закон від 16.01.2003 № 435-IV [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/435-15.

Сімейний кодекс України / Закон від 10.01.2002 № 2947-III [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2947-14.

Закон України «Про інформацію» від 02.10.1992 № 2657-XII // [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12.

Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI // [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2939-17.

Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/3855-12.

Закон України «Про основні засади розбудови інформаційного суспільства в Україні на 2007 – 2015рр» від 09.01.2007 № 537-V [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/537-16.

Закон України «Про доступ до судових рішень» від 22.12. 2005 № 3262-IV [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3262-15.

Постанова Кабінету Міністрів України від 9 серпня 1993р. № 611 «Про перелік відомостей, що не становлять комерційної таємниці» [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/611-93-%D0%BF.

Загальна декларація прав людини / ООН; Міжнародний документ від 10.12.1948 // [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_015.

Міжнародний пакт про економічні, соціальні та культурні права / ООН; Міжнародний документ від 16.12.1966 [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/995_042.

Конвенції про захист прав людини і основоположних свобод Рада Європи / Міжнародний документ від 04.11.1950 [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/995_004.

Міжнародний пакт про громадянські і політичні права ООН / Міжнародний документ від 16.12.1966 [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу :
http://zakon4.rada.gov.ua/laws/show/995_043.

Науково-практичний коментар до Закону України "Про доступ до публічної інформації" [Електронний ресурс] // Верховна Рада України : [сайт]. – Режим доступу :
http://www.president.gov.ua/docs/comment_api_final.pdf.

Азарова Т.В., Абрамов Л.К. Інформаційне забезпечення процесу вирішення соціальних проблем на місцевому рівні [Текст] / Т.В.Азарова, Л.К.Абрамов. – Кіровоград:ІСКМ, 2003 – 116 с.

Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти // За ред. Бандурки О.М.// Харків : Видавництво Університету внутрішніх справ, 2000. – с. 9.

Баранов О. А. Інформаційне право України : стан, проблеми, перспективи / О. А. Баранов – К. : Софт Прес, 2005. – 316 с.

Демкова М. Інформація, як основа інформаційного суспільства: поняття та правове регулювання / М. Демкова, М.Фігель [Електронний ресурс] // Режим доступу : http://uk.wikipedia.org

Заворотченко Т.М . Теоретико-правовий аналіз права на інформацію [Текст] / Т.М.Заворотченко // Право і суспільство. – 2010. – № 2. – С. 48 – 53.

Заєць О.В. Забезпечення реальності інформаційних прав людини і громадянина як основа інформаційної безпеки сучасної держави [Текст] / О.В.Заєць // Право і безпека : наук. журн. – 2012. – № 3. – С. 92 – 96.

Коваленко Л. П. Теоретичні проблеми розвитку інформаційного права України : монографія / Л. П. Коваленко. –Х. : Право, 2012. – 248 с.

Коліушко І.Б. Електронне урядування – шлях до ефективності та прозорості державного управління / І.Б. Коліушко, М.С. Демкова //

Інформаційне суспільство. Шлях України. – К. : Бібліотека інформаційного суспільства, 2004. – С. 138 – 143.

Копылов В.А. Информационное право // Юристъ – М. : 1997. – 472 с.

Котюжинська Т. Право на інформацію – зміни необхідні [Текст] /Т.Котюжинська // Юридичний журнал. – 2009. – № 10. – С. 45 – 48.

Марущак А.І. Інформаційне право : доступ до інформації [Текст] : навч. посіб. / А.І.Марущак. –К. : КНТ, 2007. – 532 с.

Марущак А. До питання про зміст права на інформацію [Текст] / А.Марущак // Юридичний радник. – 2006. – № 4. – С. 73 – 75.

Нестеренко О.В. Інформація в Україні : право на доступ [Текст] / О.В.Нестеренко. – Х. : Акта, 2012. – 83 с.

Політанський В.С . Принципи інформаційно-правових відносин / В.С, Політанський // Часопис Київського університету права. – 2013. – № 1. – С. 55 – 59.

Право на доступ до інформації: теорія та практика [Текст]. – Х. : Права людини, 2008. – С. 348.

Тарасенко Р.Б. Інформаційне право: навчально-методичний посібник / МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с.

Цимбалюк В. С. Основи інформаційного права України : навч. посіб. / В. С. Цимбалюк, В. Д. Гавловський, В. В. Гриценко та ін; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. – К : Знання, 2004. – 274 с.

Черешкин Д.С. Оружие, которое может быть опаснее ядерного // Независимая газета. – 1995. – № 123.

Юридична енциклопедія: в 6 т. // Редкол. : Ю.С.Шемшученко (голова редкол.) та ін. – К. : “Укр. енцикл.”, 1998 – с. 717.

## Розділ ІІ Інформаційна безпека

## Тема 7. Організаційно-правова характеристика інформаційної безпеки

### 7.1. Поняття інформаційної безпеки

Реалії сучасного інформаційного суспільств показують, що жодна сфера життя цивілізованої держави не може ефективно функціонувати без розвинутої інформаційної інфраструктури, широкого застосування апаратно-програмних засобів та мережевих технологій обробки та обміну інформації. Безліч понять і термінів інформаційної безпеки відображає широкий спектр відмінних істотних властивостей, ознак і відносин, властивих даному специфічного виду безпеки. Виділяють три групи термінів теорії інформаційної безпеки. Розглянемо перелік термінів, що входять у кожну групу.

**Терміни, які визначають наукову основу інформаційної безпеки.**

На думку авторів до цієї групи відносяться терміни, які використовуються в багатьох галузях знань і є однозначними, семантично уніфікованими і стилістично нейтральними. Це: інформація, комунікація, конфлікт, вплив, загроза, небезпека, безпека, система. Терміни цієї групи відповідають вимогам однозначності і стійкості, тобто ці терміни однозначно вживаються в одній галузі знань і зберігають свій особливий сенс у кожної іншої галузі знань, а також є загальновизнаними – вони вживаються в побуті. Однак терміну «інформація» притаманна специфічно властивість: у різних областях знань, і навіть в одній області знання він може характеризувати предмет, явище, процес та їх властивості і відносини одночасно.

**Терміни, що визначають предметну основу інформаційної безпеки.**

До другої групи належать терміни, що позначають поняття і їх співвідношення з іншими поняттями в межах інформаційної безпеки як спеціальної сфери або галузі знань. До таких відносяться: інформатика, інформатизація, інформаційна система, інформаційні технології, інформаційні процеси, інформаційний об'єкт, інформаційний ресурс, інформаційна інфраструктура, інформаційна сфера, інформаційний потенціал.

## Терміни, що визначають характер діяльності щодо забезпечення інформаційної безпеки.

До третьої групи відносяться терміни, службовці позначеннями характерних для цієї сфери предметів, явищ, процесів, їх властивостей і відносин (у тому числі сил, засобів і методів їх використання при вирішенні завдань забезпечення інформаційної безпеки). Терміни цієї групи позначають широке коло понять різного рівня: від технічного каналу витоку інформації до інформаційного протиборства. До них відносяться: інформаційне протиборство, інформаційну перевагу, інформаційна безпека, загрози інформаційній безпеці, забезпечення інформаційної безпеки, система забезпечення інформаційної безпеки, інформаційна захищеність, безпеку інформації, захист інформації, об'єкт захисту інформації, носій інформації, доступ до інформації, доступність інформації, цілісність інформації, конфіденційність інформації, несанкціонований доступ до інформації, витік інформації, канал витоку інформації, канал передачі інформації, вплив на інформацію, інформаційно-психологічний вплив, інформаційно-психологічна сфера. Важливою специфічною особливістю термінологічної системи інформаційної безпеки є її тісний зв'язок з правової лексикою. Це наслідок того факту, що інформаційна безпека давно перестала бути технічною дисципліною, частиною інформатики. У зв'язку з цим вироблення однаковості в термінології з проблеми забезпечення інформаційної безпеки створює передумови для цілеспрямованого розвитку всіх робіт з теорії інформаційної безпеки та методології захисту інформації.

Отже, **інформаційна безпека** – це стан захищеності життєво-важливих інтересів особистості, суспільства і держави в інформаційній сфері від внутрішніх та зовнішніх загроз.

### 7.2. Джерела загроз інформаційної безпеки України

Джерела загроз інформаційної безпеки України розділяються на зовнішні та внутрішні.

**До зовнішніх джерел відносяться**: діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур, спрямованих проти інтересів України в інформаційній сфері; прагнення ряду країн до домінування і ущемлення інтересів України в світовому інформаційному просторі, витіснення її з зовнішнього і внутрішнього інформаційних ринків; загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами; діяльність міжнародних терористичних організацій; збільшення технологічного відриву провідних держав світу і нарощування їх можливостей з протидії створенню конкурентоспроможних українських інформаційних технологій; діяльність космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав; порушення нормального функціонування інформаційних і телекомунікаційних систем, збереження інформаційних ресурсів, отримання несанкціонованого доступу до них.

**До внутрішніх джерел належать**: критичний стан вітчизняних галузей промисловості; несприятливий криміногенний стан, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері, отримання кримінальними структурами доступу до конфіденційної інформації, посилення впливу організованої злочинності на життя суспільства, зниження ступеня захищеності законних інтересів громадян, суспільства і держави в інформаційній сфері; недостатня координація діяльності органів державної влади з формування та реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки України; недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика; нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком

інформаційного ринку України; недостатнє фінансування заходів щодо забезпечення інформаційної безпеки України; недостатня економічна міць держави; зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки тощо.

### 7.3. Основні складові інформаційної безпеки

Інформаційна безпека багатовимірна галузь діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

З методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів. У забезпеченні інформаційної безпеки потребують різні суб'єкти інформаційних відносин, такі як: держава в цілому або окремі органи та організації; громадські або комерційні організації (об'єднання), підприємства (юридичні особи); окремі громадяни (фізичні особи). Весь спектр інтересів суб'єктів, пов'язаних з використанням інформації, можна розділити на такі категорії.

Забезпечення доступності, цілісності і конфіденційності ресурсів інформаційного середовища та підтримуючої інфраструктури.

**Доступність** – це можливість за прийнятний час отримати необхідну інформаційну послугу. Під цілісністю мається на увазі актуальність і непротиріччя інформації, її захищеність від руйнування і несанкціонованої зміни.

**Конфіденційність** – це захист від несанкціонованого доступу до інформації. В якості основних інформаційних ресурсів надалі будемо розглядати інформаційні системи і засоби комунікації.

Інформаційні системи створюються (купуються) для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитків усім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність іншим

аспектам, прийнято виділяти її як найважливіший елемент інформаційної безпеки.

можна поділити на статичну і динамічну. Засоби контролю динамічної цілісності застосовуються зокрема при аналізі потоку фінансових повідомлень з метою виявлення крадіжок, дублювання окремих повідомлень.

Конфіденційність – самий пророблений у нас в країні аспект інформаційної безпеки. Але практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем має в Україні серйозні труднощі. По-перше, відомості про технічні канали витоку інформації є закритими. Більшість користувачів позбавлені можливості скласти уявлення про потенційні ризики. По-друге, на шляху криптографії користувачів як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми.

### 7.4. Забезпечення інформаційної безпеки

Предметна галузь забезпечення інформаційної безпеки – це коло правовідносин, яке визначає правове становище різних суб'єктів та об'єктів у сфері інформаційних комунікаційних технологій – комплекс (сукупність елементів інфраструктури, на основі якої формується технологічна база інформаційних систем країн, що беруть участь в глобальному інформаційному просторі). До об'єктів правового регулювання забезпечення інформаційної безпеки відносяться: правовий режим різних елементів інформаційних комунікаційних технологій; визначення правового статусу суб'єктів з урахуванням їх спеціальною інформаційного середовища; правове забезпечення спеціальних суб'єктів, що здійснюють діяльність у сфері забезпечення інформаційної безпеки.

Основні напрямки забезпечення інформаційної безпеки: встановлення різних видів обмежень; підвищення значущості таких видів забезпечення інформаційної безпеки, як сертифікація, ліцензування, в тому числі і експертиза діяльності; встановлення процедур створення, отримання та використання

інфраструктури з обмеженим доступом; уніфікація підходів і стандартів до електронних документів; висновок, встановлення режимів службової інформації. Правове регулювання забезпечення інформаційної безпеки має здійснюватися на різних рівнях, починаючи з самого нижнього: участь громадян у забезпеченні інформаційної безпеки; забезпечення інформаційної дисципліни в корпораціях; організація підрозділів інформаційної безпеки в органах державної влади на всіх рівнях; встановлення процесуального законодавства; встановлення стандартів, що засвідчують технічну безпеку інформаційних систем; створення системи органів влади в цій галузі; вироблення угод і умов міжнародного співробітництва та забезпечення інтересів України з урахуванням позицій національної безпеки.

Шкідлива інформація – інформація, яка не є конфіденційною, але яка обумовить необхідність охорони та захисту прав і законних інтересів особистості, суспільства і держави в силу виникнення шкоди, який завдасть цим суб'єктам її поширення. Шкідливу інформацію можна розділити на групи: інформація направлена на розпалювання ненависті, ворожнечі і насильства; помилкова інформація (у тому числі недоброякісна, недобросовісна, неправдива реклама); інформація, що містить посягання на честь, добре ім'я та ділову репутацію; непристойна інформація; інформація, що надає деструктивний вплив на здоров'я людей (у тому числі технічні пристрої, що діють на психіку людей).

**Контрольні запитання для самоперевірки**

1. Дайте визначення поняттю «інформаційна безпека».
2. Назвіть основні характеристики загроз інформаційній безпеці України.
3. Які основні складові інформаційної безпеки?
4. Визначте основні напрямки забезпечення інформаційної безпеки.

## Тема 8. Система забезпечення інформаційної безпеки

### 8.1. Поняття системи забезпечення інформаційної безпеки

У найбільш загальному плані під **системою забезпечення інформаційної безпеки** розуміємо систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення.

Основами формування і функціонування системи забезпечення інформаційної безпеки є: комплексне визначення поняття інформаційної безпеки та її складових елементів, світоглядне та концептуальне закріплення у концепції, доктрині, програмах, планах та інших документах; формування і діяльність оптимальної структури системи інформаційної безпеки, аналіз функціонування її окремих елементів, організація функціонування даної системи в цілому; формування єдиного методологічного підходу, а також вироблення і прийняття єдиного цілісного і узгодженого законодавства з питань інформаційної безпеки; створення чіткого механізму, метою якого було б координування діяльності елементів системи забезпечення інформаційної безпеки на усіх рівнях державного управління; підготовка і забезпечення найкращими професійними кадрами всі складові елементи підсистеми інформаційної безпеки.

За наявності даних основ можна говорити про їх системну взаємодію, яка забезпечить створення і функціонування чіткої і надійної системи забезпечення інформаційної безпеки.

Відповідно до основ формування можна виокремити **основні функції** системи забезпечення інформаційної безпеки України.

1. Створення та забезпечення діяльності державних та недержавних органів та організацій – елементів системи забезпечення інформаційної безпеки, що включає: розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини

інформаційної безпеки, організаційної та функціональної структури системи); системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення усієї системи державного управління.

2. Управління системою інформаційної безпеки – здійснення свідомого цілеспрямованого впливу суб'єкта управління на за грози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки: розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня державного управління; здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;

оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки.

3. Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки: визначення інтересів органів державного управління в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики; діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів.

4. Міжнародне співробітництво в сфері інформаційної без пеки: розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки; входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України; участь у роботі керівних, виконавчих та забезпечуючи підрозділів цих структур (організацій), спільне проведення планових заходів.

Звичайно, що перелік функцій не є вичерпним, водночас за їх наявності можна говорити про формування певної підсистеми, мета функціонування якої корелюватиме із загальною метою функціонування системи національної безпеки. Актуальним в контексті розглядуваних проблем вбачається проаналізувати зміст та призначення системи забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек.

**Метою** забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки. Структурна зв'язаність елементів системи забезпечення інформаційної безпеки є істотною її якісною характеристикою і розрив зв'язків між цими елементами може призвести до зникнення самої системи, а отже актуалізується питання забезпечення структурної єдності даної системи.

Так, наприклад, захищеність Кабінету Міністрів України і незахищеність місцевої адміністрації міста Києва у своїй сукупності не утворять стан захищеності усієї системи інформаційної безпеки органів державного управління.

Таким чином, суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, вживаючи при цьому відповідні, визначені законом, адміністративно-правові форми та методи. У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють струнку організаційно-функціональну систему, об'єднану як системою владно-

розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки. Отже, об'єктами системи забезпечення інформаційної безпеки України є: інтереси органів державного управління в інформаційній сфері; система органів державного управління, а також їх компетентні особи і відносини між ними (суспільні відносини в інформаційній сфері); власне система забезпечення інформаційної безпеки України.

### 8.2. Рівні інформаційної безпеки

У системі забезпечення інформаційної безпеки основними елементами вважаємо перелік її рівнів. Аналіз джерел засвідчує, що науковці пропонують розглядати такі рівні інформаційної безпеки: нормативно-правовий рівень – закони, нормативно-правові акти тощо; адміністративний рівень – дії загального характеру, які вживаються органами державного управління; процедурний рівень – конкретні процедури забезпечення інформаційної безпеки; програмно-технічний рівень – конкретні технічні заходи забезпечення інформаційної безпеки. Розглянемо дещо детальніше кожний з цих рівнів. На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному рівні здійснюється ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності. На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На технологічному рівні здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у

форматі координації дій органів державного управління, які пов'язані між собою однією метою. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і / або карається суспільством, тому, що так чинити не прийнято.

На законодавчому рівні розрізняють дві групи заходів: - заходи, спрямовані на створення і підтримку в суспільстві негативного (у тому числі із застосуванням покарань) ставлення до порушень і порушників інформаційної безпеки (назвемо їх заходами обмежувальної спрямованості); - направляючі і координуючі заходи, що сприяють підвищенню освіченості суспільства в галузі інформаційної безпеки, що допомагають у розробці та поширенні засобів забезпечення інформаційної безпеки (заходи творчої спрямованості). Найважливіше (і, ймовірно, найважче) на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, так як на практиці, крім інших негативних моментів, це веде до зниження інформаційної безпеки.

До адміністративного рівня інформаційної безпеки відносяться дії загального характеру. Головна мета заходів адміністративного рівня – сформувати програму робіт в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ. Основою програми є політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації має усвідомити необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів. Політика безпеки будується на основі аналізу ризиків, які

визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані та стратегія захисту визначена, складається програма забезпечення інформаційної безпеки. «Політика безпеки» (є не зовсім точним перекладом англійського словосполучення «security policy»), має на увазі не окремі правила або їх набори, а стратегію організації в галузі інформаційної безпеки. Політика безпеки – сукупність документованих рішень, прийнятих керівництвом організації і спрямованих на захист інформації та асоційованих з нею ресурсів.

Процедурний рівень, орієнтований на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки, і вони ж виявляються головною загрозою, тому «людський фактор» заслуговує особливої уваги. Слід усвідомити ту ступінь залежності від комп'ютерної обробки даних, в яку потрапило сучасне суспільство. Акцент слід робити не на військовому чи кримінальному боці справи, а на цивільних аспектах, пов'язаних з підтриманням нормального функціонування апаратного та програмного забезпечення, тобто концентруватися на питаннях доступності та цілісності даних.

Програмно-технічний рівень, тобто рівень, спрямований на контроль комп'ютерних сутностей - обладнання, програм та / або даних, утворюють останній і найважливіший рубіж інформаційної безпеки. Наголошуємо, що збиток наносять в основному дії легальних користувачів, по відношенню до яких процедурні регулятори малоефективні. Головні вороги – некомпетентність і неакуратність при виконанні службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти.

### 8.3. Загрози інформаційної безпеки

**Загрози інформаційної безпеки** є сукупністю негативних чинників (умов), які ускладнюють (унеможливлюють) реалізацію інформаційних інтересів особи, суспільства та держави.

У питанні про класифікацію зазначених загроз вчені демонструють різні підходи. Окремі з них не подають саму класифікацію, а лише наголошують на малопродуктивності ізольованого, не комплексного виявлення загроз безпеці та пропонують їх розглядати в комплексі.

Необхідність у розробленні поняття «загроза» визначається: 1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки; 2) недостатньою розробленістю родового поняття «загроза» і питань його відмежування від інших споріднених понять, таких, як «небезпека», «виклик», «ризик», і відповідно видового «інформаційна загроза» і його відмежування від таких понять, як «інформаційна війна», «інформаційне протиборство», «інформаційний тероризм»; 3) наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки; 4) можливістю на підставі теоретичних розробок даного апарату формувати адекватну систему моніторингу та управління загрозами та небезпеками в інформаційній сфері.

Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто від находження джерела актуалізації певних подій у загрози характеризується таким елементом, як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю відповідно до теорії множин є не вичерпними, а отже і не можуть бути піддані повному описові.

Інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання, вважаємо, що можна виділити такі **види загроз інформаційній**

**безпеці:** розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

**До системи загроз інформаційній безпеці відносимо:**

– за ступенем небезпеки – особливо небезпечні, небезпечні;

– за можливістю дії – реальні, потенційні;

– за масштабами дії – національні, локальні, індивідуальні;

– за тривалістю дії – тимчасові, постійні;

– за характером впливу – прямі, безпосередні, опосередковані;

– за терміном дії – довгострокові, середньострокові, короткострокові, поточні;

– за сферою інформаційної діяльності – загрози у зовнішньополітичній сфері; у воєнній сфері; у внутрішньополітичній сфері; в економічній сфері; у соціальній та гуманітарній сферах; у науково-технологічній сфері; в екологічній сфері.

**Контрольні запитання для самоперевірки**

1. Дайте визначення поняттям «загроза», «небезпека».
2. Назвіть основні характеристики загроз інформаційній безпеці України.
3. Визначте види загроз за певними критеріями.

## Тема 9. Інформаційна безпека особистості

### 9.1. Загальна характеристика інформаційної безпеки особистості

**Інформаційна безпека особистості** – стан та умови життєдіяльності особистості, при яких реалізуються її інформаційні права і свободи. Життєво важливі інтереси особистості в інформаційній сфері наступні. Дотримання та реалізація конституційних прав на пошук, отримання прав і поширення інформації. Реалізація прав громадянина на недоторканність приватного життя. Використання інформації в інтересах не закріпленої законом діяльності, спрямованої на фізичний, духовний, інтелектуальний розвиток. Захист прав на об'єкти інтелектуальної власності. Забезпечення прав громадянина на захист свого здоров'я від неусвідомлюваної шкідливої

інформації. Загрози інтересам особистості в інформаційній сфері. Застосування нормативно-правових актів, що суперечать конституційним правам громадян. Протидія, в тому числі з боку кримінальних структур, реалізація громадянами прав на недоторканність приватного життя. Порушення прав громадян в галузі масової інформації. Протиправне застосування спеціальних засобів, що впливають на свідомість. Маніпулювання інформацією (дезінформація; приховування інформації; спотворення інформації).

### 9.2. Інформаційно-психологічна безпека

У відношенні людини держава повинна забезпечувати інформаційно-психологічну безпеку. **Інформаційно-психологічна безпека** – стан захищеності окремих осіб та (або) груп осіб від негативних інформаційно-психологічних впливів і пов'язаних з цим інших життєво важливих інтересів особистості, суспільства і держави в інформаційній сфері.

**Основними принципами забезпечення інформаційно-психологічної безпеки є**: адекватність заходів безпеки існуючим загрозам; державна монополія на розробку і виробництво спеціальних засобів інформаційно-психологічного впливу; гласність і цивільний контроль за забезпеченням інформаційно-психологічної безпеки; обов'язковість участі громадських організацій у діяльності щодо забезпечення інформаційно-психологічної безпеки.

**До основних загроз інформаційно-психологічної безпеки належить** можливість настання негативних наслідків для суб'єктів, що піддаються інформаційно-психологічному впливу, які можуть виражатися у таких формах: заподіяння шкоди здоров'ю людини; блокування на неусвідомлюваному рівні свободи волевиявлення людини, штучне прищеплення йому синдрому залежності; маніпуляція суспільною свідомістю; руйнування єдиного інформаційного і духовного простору України, традиційних устоїв суспільства і

суспільної моралі, а також порушенні інших життєво важливих інтересів особистості, суспільства і держави.

**Джерелами загроз інформаційно-психологічної безпеки є:** фізичні особи, які володіють природними здібностями впливу на психіку людей; розробка програмних і технічних засобів; релігійні й інші групи; антропогенні зони; геопатогенні зони. Ці джерела можуть спричинити: заподіяння шкоди здоров'ю; блокування на неусвідомлюваному рівні волевиявлення людини; маніпулювання суспільною свідомістю; руйнування єдиного інформаційного простору.

**Державна система забезпечення інформаційно-психологічної безпеки здійснює такі функції**: виявлення та облік суб'єктів, що здійснюють негативні інформаційно-психологічні впливу, і контроль за їх діяльністю; ведення моніторингу негативних інформаційно-психологічних впливів; припинення негативних інформаційно-психологічних впливів; підготовку кадрів для забезпечення інформаційно-психологічної безпеки із залученням недержавних освітніх і наукових організацій; розробку та вдосконалення методів і засобів виявлення та нейтралізації негативних інформаційно-психологічних впливів, реабілітації осіб, що постраждали від такого впливу; організацію реабілітації осіб, постраждалих від негативних інформаційно-психологічних впливів; організацію системи ліцензування, сертифікації, експертизи та контролю у сфері інформаційно-психологічної безпеки; організацію розробки і прийняття стандартів у сфері інформаційно-психологічної безпеки; розробку спеціальних засобів і методів інформаційно-психологічних впливів; інформування громадськості про діяльність осіб і організацій, порушують законодавство в галузі інформаційно-психологічної безпеки; сприяння розробці та прийняттю норм міжнародного права в галузі забезпечення інформаційно-психологічної безпеки.

### 9.3. Інформаційно-ідеологічна безпеку

Ідеологічна безпека має з інформаційною спільність по предмету правового та організаційного регулювання (інформація), однак якщо інформаційне право покликане регулювати суспільні відносини з приводу створення, поширення, зберігання, переробки і споживання інформації, визначаючи останню як явище статичне, то інститут ідеологічної безпеки, регулюючи ті ж відносини, розглядає інформацію як явище динамічне, тобто принципово важливою характеристикою тут вже є ступінь і характер її впливу на свідомість людей, а не її ступінь захищеності, авторство і т.п. Звідси вже зовсім різні методи. Вони в інституту ідеологічної безпеки особливі: соціальна реклама, організаційне та фінансове супровід творчих проектів, публічне державне визнання і проголошення, деякі методи ведення інформаційної війни тощо.

Таким чином, слід розділити інформаційну безпеку на інформаційно-ідеологічну та інформаційно-технічну. При цьому під **інформаційно-технічною безпекою** слід розуміти "захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести нанесенням шкоди власникам або користувачам інформації і підтримуючої інфраструктури", а під **інформаційно-ідеологічної** (далі – ідеологічної) безпекою – захищеність суспільства і особистості від навмисного або ненавмисного інформаційного впливу, що має результатом порушення прав і свобод людини і громадянина в галузі створення, споживання та поширення інформації, користування інформаційною інфраструктурою і ресурсами, що суперечить моральним і етичним нормам, роблять деструктивний вплив на суспільство, особистість, що мають негласний (неусвідомлений) характер. Способи забезпечення ідеологічної безпеки можна класифікувати залежно від того, чи підлягає застосуванню імперативний або диспозитивний метод. Якщо говорити про диспозитивних методах, то до їх числа відносяться дві групи – організаційні та інформаційно-пропагандистські.

До числа організаційних можна віднести: організаційний супровід творчих проектів, адресне фінансування, організацію взаємодії державних органів, надання аналітичних узагальнень, організацію різного роду акцій, напрямок підприємців за кордон для підвищення кваліфікації та навчання менеджменту тощо.

Інформаційно-пропагандистські прийоми в загальному відносяться до методики проведення інформаційної війни і так званим технологіям "піар". Доцільним представляється розробка комплексних програм впливу, які можна, в свою чергу, поділити на нейтралізуючі негативний вплив певного джерела; пов'язані з економічним стимулюванням суспільства; військові програми; освітні; культурно-просвітницькі; наукові; демографічні; спеціальні тактичні інші.

За сферою дії можна виділити міжнародні, регіональні, локальні програми. По спрямованості і тривалості – стратегічні (довгострокові), оперативні (середньострокові) і тактичні (короткострокові). Дана класифікація передбачає наявність базової всеосяжною і взаємозалежної програми.

Загрози національній ідеологічної безпеки можна класифікувати по різних підставах на внутрішні і зовнішні, навмисні (організовані) і ненавмисні (стихійні), явні та латентні (приховані) і т.п. Представляється доцільним розташувати їх за ступенем суспільної небезпеки в порядку зменшення: ворожа діяльність спеціальних органів іноземних держав; деструктивна організована цілеспрямована діяльність внутрішньодержавних організацій; аналогічна діяльність міжнародних недержавних організацій (транснаціональних корпорацій і т.п.); гострі соціальні суперечності, викликані політичним, економічним або іншим кризою; відсутність мінімального контролю за інформаційними потоками з метою забезпечення морального здоров'я населення; монополізованості ЗМІ; застосування некоректних методів ідеологічного впливу; масове дезінформування в цілях спотворення громадської думки; застосування всередині країни прийомів, характерних для

міждержавного інформаційного протиборства або психологічної війни з істотним порушенням прав і свобод людини і громадянина; створення і функціонування на території України релігійних сект деструктивного толку і інших подібних організацій, практикуючих вплив на психіку людини, що спонукає його до здійснення антисоціальних вчинків; відсутність у більшості населення ціннісних орієнтацій, ідеалів, спонукальних стимулів до активної діяльності (ідеології); інші загрози.

**Контрольні запитання для самоперевірки**

1. Дайте визначення поняттю «інформаційна безпека особистості»
2. Що розуміють під інформаційно-психологічною безпекою?
3. Які загрози належать до інформаційно-психологічної безпеки ?
4. Що розуміють під інформаційно-технічною безпекою?
5. Що розуміють під інформаційно-ідеологічною безпекою?

## Тема 10. Інформаційна безпека суспільства

### 10.1. Загальна характеристика інформаційної безпеки суспільства

**Інформаційна безпека суспільства** – захист економічних, соціальних, міжнародних і духовних цінностей з використанням інформаційних засобів від зовнішніх і внутрішніх загроз. Життєво важливі інтереси суспільства в інформаційній сфері. Забезпечення інтересів суспільства. Побудова прав держави. Побудова інформаційного суспільства. Збереження моральних цінностей суспільства. Запобігання маніпулювання масовою свідомістю. Пріоритетний розвиток сучасних інформаційних технологій. Інформаційна безпека суспільства забезпечується його захистом від шкідливих інформаційних впливів в ході інформаційної війни проти країни, яка переслідує в ставленні суспільства такі основні цілі: тактичну – нав'язати свою політичну волю через ідеологічну, психологічну обробку народу, армії, військово-політичного керівництва країни в інтересах створення необхідного громадської думки; стратегічну – змінити спосіб життя, роз'єднати народ, знищити

морально-політичний потенціал суспільства і зруйнувати державу зсередини шляхом ідеологічної революції, руйнування національної самосвідомості, розмивання почуття патріотизму, культури, традицій, історичної пам'яті, підриву духовно-етичних засад. Шкідливий інформаційний вплив на суспільство реалізується в основному через ЗМІ, у тому числі електронні комунікації, шляхом створення та впровадження штампів, доступних для розуміння людини, гри на почуттях страху, надії, роздратування, що викликають стан агресії або безвиході, прагнення піти з реального світу, замінити його традиційно штучним (алкоголізм, наркоманія, прихід в деструктивні секти) або віртуальним (телевізійний, комп'ютерний), посилення соціально-політичних, економічних і духовних колізій, наростання, закріплення і розвиток психологічної та психічної напруженості, зростання агресивності, злочинності, зниження самоконтролю серед молоді, різку активізацію ірраціональної сфери суспільної свідомості, дестабілізацію соціальної спадкоємності поколінь, втрату культурної спадщини, прояв бездуховності та аморальності, підвищення злочинності в суспільстві й інші наслідки.

### 10.2. Загрози інформаційної безпеки суспільства

До загроз інформаційної безпеки суспільства відносяться: невиконання вимог закону; дезорганізація і руйнування накопичення та збереження інформації; посилення залежності суспільного життя від зарубіжних інфраструктур; активізація різного роду релігійних сект. Діяльність сект містить в собі контроль свідомості своїх членів, який включає: контроль поведінки; контроль мислення; контроль інформації; контроль емоцій; зниження духовної моральності, творчого потенціалу населення України; збільшення відтоку фахівців за кордон; порушення прав у сфері обігу інформації (витік, перехоплення, розкрадання, нав'язування неправдивої інформації); порушення правил в галузі функціонування інформаційної системи; порушення правил в галузі використання засобів забезпечення

інформаційної безпеки: вплив на парольні ключі системи; використання несертифікованих інформаційних технологій.

Найбільшу небезпеку в сфері внутрішньої політики представляють наступні загрози інформаційної безпеки України: порушення конституційних прав і свобод громадян, що реалізуються в інформаційній сфері; недостатнє правове регулювання відносин у галузі прав різних політичних сил на використання засобів масової інформації для пропаганди своїх ідей; поширення дезінформації про політику України, діяльності органів державної влади, події, що відбуваються в країні і за кордоном; діяльність громадських об'єднань, спрямована на насильницьку зміну основ конституційного ладу і порушення цілісності країни, розпалювання соціальної, расової, національної та релігійної ворожнечі, на поширення цих ідей у засобах масової інформації. Основними заходами в галузі забезпечення інформаційної безпеки України у сфері внутрішньої політики є: створення системи протидії монополізації вітчизняними та зарубіжними структурами складових інформаційної інфраструктури, включаючи ринок інформаційних послуг та засоби масової інформації; активізація контрпропагандистської діяльності, спрямованої на запобігання негативних наслідків поширення дезінформації про внутрішню політику України.

**Контрольні запитання для самоперевірки**

1. Розкрийте взаємозв'язок між поняттями «політика», «інформаційна політика», «політика інформатизації», «політика інформаційної безпеки».

2. Дайте визначення державно-правового механізму інформаційної безпеки? В чому полягають його особливості.

3. Які основні напрями державної політики в інформаційній сфері закріплені законодавчо?

4. Назвіть особливості української інформаційної політики.

5. Які основні нормативно-правові акти регулюють суспільні відносини інформаційної політики України? Розкрийте основні положення.

## Тема 11. Інформаційна безпека держави

### 11.1. Загальна характеристика інформаційної безпеки держави

**Інформаційна безпека держави** – захист конституційного ладу, суверенітету, територіальної цілісності з точки зору інформаційних засобів. Життєво важливі інтереси держави. Створення цілей для реалізації інтересів особистості і суспільства в інформаційній сфері. Формування інститутів громадського контролю органів державної влади. Безумовне забезпечення законності та правопорядку. Створення умов для розвитку власної інформаційної інфраструктури. Формування системи підготовки та реалізації рішень органів державної влади, що забезпечують національні інтереси країни. Захист державної інформаційної системи та інформаційних ресурсів (захист державної таємниці). Захист єдиного інформаційного простору країни. Поділ рівноправного і взаємного міжнародного співробітництва. Руйнування єдиного інформаційного простору України. Витіснення українських інформаційних агентств та засобів масової інформації з внутрішнього інформаційного ринку. Монополізація інформаційного ринку. Блокування діяльності державних засобів масової інформації з інформування української, зарубіжної аудиторії. Послаблення ролі української мови як державної мови України. Цілеспрямоване втручання і проникнення в діяльність і розвиток інформаційних систем. Низька ефективність інформаційного забезпечення державної політики (дефіцит кадрів, відставання інформаційних систем від міжнародних стандартів). Останнім часом зловживання свободою масової інформації є одним з головних внутрішніх джерел загроз інформаційній безпеці України. На думку експертів, близько 40% розвідувальної інформації виходить у процесі аналітичної обробки відкритих матеріалів, включаючи друковані та електронні ЗМІ. На сьогоднішній день зміна загроз "холодної війни" погрозами

"інформаційної війни" суттєво підвищує значення інформаційної безпеки в системі національної безпеки держави, обумовлює розширення її змісту. Втрата державного контролю над українськими комунікаціями може привести до втрати національної незалежності.

### 11.2. Загрози безпеки держави в інформаційній сфері

Інформаційна безпека визначається тим, наскільки кожен із суб'єктів у відповідності зі своєю позицією та інтересами має можливість через засоби масової інформації та телекомунікацій вільно шукати, одержувати і поширювати достовірну інформацію. Суспільство не може відчувати себе в безпеці, якщо воно отримує препаровану, керовану інформацію. Невід'ємним атрибутом розвиненого демократичного суспільства має бути дотримання законних прав особистості, суспільства і держави щодо захисту інформації обмеженого доступу. Правова держава не є просто держава, що дотримується закони. Це суспільство і держава, що визнають право як історично розвивається в суспільній свідомості, що розширюється міру свободи і справедливості, виражену саме в законах, підзаконних актах і практиці реалізації прав, свобод і законних інтересів громадян.

До найбільш важливих об'єктів забезпечення інформаційної безпеки нашої країни у сфері зовнішньої політики належать: інформаційні ресурси органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях; блокування діяльності українських засобів масової інформації з роз'яснення зарубіжної аудиторії цілей і основних напрямів державної політики України, її думки з соціально значимих подій українського і міжнародного життя.

Із зовнішніх загроз інформаційної безпеки України у сфері зовнішньої політики найбільшу небезпеку становлять: інформаційний вплив іноземних

політичних, економічних, військових та інформаційних структур на розробку і реалізацію стратегії зовнішньої політики України; поширення за кордоном дезінформації про зовнішню політику України; порушення прав українських громадян і юридичних осіб в інформаційній сфері за кордоном; спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях.

З внутрішніх загроз інформаційної безпеки України у сфері зовнішньої політики найбільшу небезпеку становлять: порушення встановленого порядку збирання, обробки, зберігання та передачі інформації в органах виконавчої влади, що реалізують зовнішню політику України, на підвідомчих їм підприємствах, в установах та організаціях; інформаційно-пропагандистська діяльність політичних сил, громадських об'єднань, засобів масової інформації та окремих осіб, що спотворює стратегію і тактику зовнішньополітичної діяльності України; недостатня інформованість населення про зовнішньополітичну діяльність України.

Основними заходами щодо забезпечення інформаційної безпеки України у сфері зовнішньої політики є: розробка основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу нашої країни; розробка та реалізація комплексу заходів щодо посилення інформаційної безпеки інформаційної інфраструктури органів виконавчої влади, що реалізують зовнішню політику України, вітчизняних представництв та організацій за кордоном, представництв України при міжнародних організаціях; створення українськими представництвам та організаціям за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику України; вдосконалення інформаційного забезпечення роботи з протидії порушенням прав і свобод громадян і юридичних осіб за кордоном. Забезпечення інформаційної безпеки України у сфері духовного

життя має на меті захист конституційних прав і свобод людини і громадянина, пов'язаних з розвитком, формуванням і поведінкою особистості, свободою масового інформування, використання культурного, духовно-морального спадщини, історичних традицій і норм суспільного життя, із збереженням культурного надбання народу, реалізацією конституційних обмежень прав і свобод людини і громадянина в інтересах збереження та зміцнення моральних цінностей суспільства, традицій патріотизму і гуманізму, здоров'я громадян, культурного та наукового потенціалу України, забезпечення обороноздатності і безпеки держави. До числа основних об'єктів забезпечення інформаційної безпеки України у сфері духовного життя відносяться: гідність особи, свобода совісті, включаючи право вільно вибирати, мати і поширювати релігійні й інші переконання і діяти відповідно до них, свобода думки і слова (за винятком пропаганди чи агітації, що збуджують соціальну, расову, національну чи релігійну ненависть і ворожнечу), а також свобода літературної, художньої, наукової, технічної та інших видів творчості, викладання; свобода масової інформації; недоторканність приватного життя, особиста і сімейна таємниця. Найбільшу небезпеку в сфері духовного життя представляють наступні загрози інформаційної безпеки України: деформація системи масового інформування як за рахунок монополізації засобів масової інформації, так і за рахунок неконтрольованого розширення сектора зарубіжних засобів масової інформації у вітчизняному інформаційному просторі; погіршення стану і поступовий занепад об'єктів української культурної спадщини, включаючи архіви, музейні фонди, бібліотеки, пам'ятки архітектури, зважаючи недостатнього фінансування відповідних програм і заходів; можливість порушення суспільної стабільності, нанесення шкоди здоров'ю та життю громадян внаслідок діяльності релігійних об'єднань, які проповідують релігійний фундаменталізм, а також тоталітарних релігійних сект; використання зарубіжними спеціальними службами засобів масової інформації, що діють на території України, для завдання збитків обороноздатності країни і безпеки держави, поширення

дезінформації; нездатність сучасного громадянського суспільства України забезпечити формування у підростаючого покоління і підтримка в суспільстві суспільно необхідних моральних цінностей, патріотизму та громадянської відповідальності за долю країни. Основними напрямками забезпечення інформаційної безпеки України у сфері духовного життя є: розвиток в нашій країні основ громадянського суспільства; створення соціально-економічних умов для здійснення творчої діяльності і функціонування закладів культури; вироблення цивілізованих форм і способів громадського контролю за формуванням у суспільстві духовних цінностей, що відповідають національним інтересам країни, вихованням патріотизму та громадянської відповідальності за її долю; вдосконалення законодавства України, що регулює відносини в галузі конституційних обмежень прав і свобод людини і громадянина; державна підтримка заходів щодо збереження та відродження культурної спадщини; формування правових і організаційних механізмів забезпечення конституційних прав і свобод громадян, підвищення їх правової культури в інтересах протидії свідомому чи ненавмисному порушенню цих конституційних прав і свобод у сфері духовного життя; розробка дієвих організаційно-правових механізмів доступу засобів масової інформації та громадян до відкритої інформації про діяльність органів державної влади та громадських об'єднань, забезпечення достовірності відомостей про соціально значимі події суспільного життя, які розповсюджуються через засоби масової інформації; розробка спеціальних правових та організаційних механізмів недопущення протиправних інформаційно-психологічних впливів на масову свідомість суспільства, неконтрольованої комерціалізації культури і науки; раціональне використання накопичених суспільством інформаційних ресурсів, що становлять національне надбання; введення заборони на використання ефірного часу в електронних засобах масової інформації для прокату програм, що пропагують насильство і жорстокість, антигромадську поведінку.

**Контрольні запитання для самоперевірки**

1. Що розуміють під інформаційною безпекою держави?

2. Які заходи щодо забезпечення інформаційної безпеки України у сфері зовнішньої політики ви знаєте?

3. Які основні напрямки забезпечення інформаційної безпеки України у сфері духовного життя?

## Тема 12. Інформаційна безпека в глобальному інформаційному просторі

### 12.1. Поняття глобального інформаційного простору

Матеріальним підтвердженням формування інформаційного глобального простору служить Internet, але він не єдиний фактор формування інформаційної цивілізації. Забезпечення безпеки інформації на світовому рівні – запорука у розвитку економіки та культурної спадщини всіх країн і народів. Під впливом глобалізації правові механізми впливу на суспільство розмиваються. Це обумовлено іншими територіальними просторовими умовами, самостійністю окремо взятої людини від соціального середовища, розвитком ідей "відкритого суспільства".

**Глобальний інформаційний простір** – сукупність інформаційних ресурсів та інформаційної інфраструктури, що дозволяє на основі єдиних принципів і за загальними правилами забезпечувати безпечний інформаційний взаємодія держав, організацій і громадян при їх рівнодоступності до відкритих інформаційних ресурсів, а також максимально повне задоволення їх інформаційних потреб при збереженні балансу національних та міжнародних інтересів. Об'єкти глобального інформаційного простору: інформаційні ресурси; інформаційна інфраструктура: а) інформаційні телекомунікаційні структури; б) інформаційні технології; в) системи ЗМІ; г) організаційна структура (органи влади). Глобальний інформаційний простір України включає: інформаційний простір органів державної влади; інформаційні телекомунікації системи держави (МНС, в силових структурах); державні інформаційні ресурси

– правова інформація, інформація про діяльність органів влади, інформація про надзвичайні ситуації, інформація, що представляє собою культурну цінність і спадщина, відкрита інформація про підприємства, державний інформаційний регістр; інформаційно-управлінську систему органів державної влади – є тільки у тих органів державної влади, які володіють розвиненою територіальної інфраструктурою (система МВС). Глобальний інформаційний простір може створюватися недержавними приватними органами чи громадянами.

## 12.2. Забезпечення безпеки у глобальному інформаційному просторі

Фактори, що впливають на правове регулювання глобального інформаційного простору: особливості макроекономічної політики держави; ідеологія формування інформаційного суспільства; специфіка чинного законодавства; особливості менталітету, національно-культурні особливості. Основні напрямки розвитку інформаційної безпеки глобального інформаційного простору. Визначення порядку доступу до інформації при гуманному використанні інформації. Визначення доступу до інформації у разі використання інформації на шкоду людині. Практика показала, що майже марно встановлювати порядок роботи з отримання та використання інформації через Internet; відповідальність за використання неперевіреної і часто недостовірної інформації ніхто не несе, як і за порушення авторських і суміжних прав. Найбільш ефективним може стати встановлення відповідальності при введенні інформації в Internet (встановлення порядку розповсюдження службової інформації, інформація авторського походження, офіційна та довідкова інформація). Основними об'єктами забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах є: інформаційні ресурси, що містять відомості, віднесені до державної таємниці, та конфіденційну інформацію; засоби і системи інформатизації (засоби обчислювальної техніки,

інформаційно-обчислювальні комплекси, мережі та системи), програмні засоби (операційні системи, системи управління базами даних, інше загальносистемне і прикладне програмне забезпечення), автоматизовані системи управління, системи зв'язку та передачі даних, здійснюють прийом, обробку, зберігання та передачу інформації обмеженого доступу, їх інформативні фізичні поля; технічні засоби і системи, що обробляють відкриту інформацію, але розміщені в приміщеннях, в яких обробляється інформація обмеженого доступу, а також самі приміщення, призначені для обробки такої інформації; приміщення, призначені для ведення закритих переговорів, а також переговорів, в ході яких оголошуються відомості обмеженого доступу. Основними загрозами інформаційній безпеці України у загальнодержавних інформаційних і телекомунікаційних системах є: діяльність спеціальних служб іноземних держав, злочинних співтовариств, організацій і груп, протизаконна діяльність окремих осіб, спрямована на отримання несанкціонованого доступу до інформації та здійснення контролю за функціонуванням інформаційних і телекомунікаційних систем; вимушене чинності об'єктивного відставання вітчизняної промисловості використання при створенні і розвитку інформаційних і телекомунікаційних систем імпортних програмно-апаратних засобів; порушення встановленого регламенту збору, обробки і передачі інформації, навмисні дії і помилки персоналу інформаційних і телекомунікаційних систем, відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах; використання несертифікованих відповідно до вимог безпеки засобів і систем інформатизації та зв'язку, а також засобів захисту інформації та контролю їх ефективності; залучення до робіт зі створення, розвитку та захисту інформаційних і телекомунікаційних систем організацій і фірм, що не мають державних ліцензій на здійснення цих видів діяльності. Основними напрямками забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах є: запобігання перехоплення інформації з

приміщень і з об'єктів, а також інформації, що передається каналами зв'язку за допомогою технічних засобів; виключення несанкціонованого доступу до оброблюваної або що зберігається в технічних засобах інформації; запобігання витоку інформації технічними каналами, що виникає при експлуатації технічних засобів її обробки, зберігання та передачі; запобігання спеціальних програмно-технічних впливів, що викликають руйнування, знищення, перекручення інформації або збої в роботі засобів інформатизації; забезпечення інформаційної безпеки при підключенні загальнодержавних інформаційних і телекомунікаційних систем до зовнішніх інформаційних мереж, включаючи міжнародні; забезпечення безпеки конфіденційної інформації при взаємодії інформаційних і телекомунікаційних систем різних класів захищеності; виявлення впроваджених на об'єкти і в технічні засоби електронних пристроїв перехоплення інформації. Основними організаційно-технічними заходами щодо захисту інформації в загальнодержавних інформаційних і телекомунікаційних системах є: ліцензування діяльності організацій у сфері захисту інформації; атестація об'єктів інформатизації з виконання вимог забезпечення захисту інформації при проведенні робіт, пов'язаних з використанням відомостей, що становлять державну таємницю; сертифікація засобів захисту інформації та контролю ефективності їх використання, а також захищеності інформації від витоку по технічних каналах систем і засобів інформатизації та зв'язку; введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту; створення і застосування інформаційних і автоматизованих систем управління в захищеному виконанні.

**Контрольні запитання для самоперевірки**

1. Поняття глобального інформаційного простору
2. Перерахуйте об'єкти глобального інформаційного простору
3. Які фактори впливають на правове регулювання глобального інформаційного простору?

4. Які основні напрямки забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах ви знаєте?

**Література до ІІ розділу**

1. Конституція України [Текст] : офіц. текст : [прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. із змінами: станом на 1 січня 2013 р.]. – К. : Мін-во Юстиції України, 2013. – 124 с.

2. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюція 60/45, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй від 08.12.2005 № 60/45.

3. Про банки і банківську діяльність: Закон України від 7 грудня 2000 р. № 2121-ПІ // Відомості Верховної Ради. – 2001. – № 5-6. – Ст. 30.

4. Про державну таємницю: Закон України від 21 січня 1994 р. № 3855-XII // Відомості Верховної Ради. – 1994. – № 16. – Ст. 93.

5. Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради. – 1992. – № 48. – Ст. 650.

6. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 р. № 3759-ХН // Відомості Верховної Ради. – 1994. – № 10. – Ст.43.

7. Про захист суспільної моралі: Закон України // Відомості Верховної Ради України. – 2004. – Ст. 192.

8. Про друковані засоби масової інформації (пресу) в Україні: Закон України // Відомості Верховної Ради України. – 1993. – Ст. 1.

9. Про бібліотеки і бібліотечну справу: Закон України // Відомості Верховної Ради України. – 1995. – Ст.4.

10. Про авторське право і суміжні права: Закон України // Відомості Верховної Ради України. – 1994. – Ст.64.

11. Про внесення змін до закону України «Про Національний архівний фонд і архівні установи»: Закон України // Відомості Верховної Ради України. – 2002. – Ст.81.

12. Про інформаційні агентства: Закон України // Відомості Верховної Ради

України, від 28.02.1995 № 74/95-ВР.

13. Про основи національної безпеки України: Закон України від 19.06.03 р. за № 964-ІУ // Відомості Верховної Ради. – 2003. – №39. –Ст. 351.

14. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 9 серпня 1993 р. – № 611.

15. Про стратегію національної безпеки України: Указ Президента України // Стратегічна панорама. – 2007. – № 1.

16. Проект Доктрини інформаційної безпеки України (РНБО України).

17. Про національну комісію з утвердження свободи слова та розвитку інформаційної галузі: Указ Президента України від 6 червня 2006 р., № 493/2006 // Уряд, кур'єр. – 2006. – 21 черв.

18. Іро основні засади розвитку інформаційною суспільства в Україні на 2007-2015 роки: Закон України // Уряд, кур'єр. – 2007. – 14 лют.

19. Про доступ до публічної інформації: Закон України // Урядовий кур'єр. – 15.02.2011. – № 28.

20. Про захист персональних даних: Закон України // Голос України. – 16.09.2010. – № 172.

21. Про затвердження Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій «Сто відсотків» на період до 2015 року: Постанова Кабінету Міністрів України від 13.04.2011 № 494 // Офіційний вісник України. – № 35. – Ст. 1462.

22. Бачило И.Л. Информационное право: актуальные проблемы теории и практики / И.Л. Бачило. – М.: Юрайт. – 2013. – 435 с.

23. Брижко В.М. Теорія і практика інформаційного права: методологія кодифікації інформаційного законодавства України / В.М. Брижко // Правова інформатика. – 1(37)/2013. – С.70.

24. Василюк В.Я. Інформаційна безпека держави: курс лекцій / В.Я. Василюк, С.О. Климчук. – К.: КНТ, Видавничий дім «Скіф», 2013. –136 с.

25. Задихайло О.А. Організація управління культурою в Україні (адміністративно-правовий аспект): дис. канд. юрид. наук: 12.00.07 / Задихайло Олена Анатоліївна; Національна юридична академія України ім. Ярослава Мудрого. – Х., 2005. – 20 с.
26. Защита информации в системах ее передачи и обработки / [Киселев В.Д., Есиков О.В., Кислицын А.С.]. – 2-е изд. – М.: Солид, 2013. – 202 с.
27. Інформаційне право (основи теорії і практики) / В.С. Цимбалюк. – К.: Освіта України, 2010. – 388 с.
28. Ліпкан В.А. Національна безпека України: навчальний посібник / В.А. Ліпкан. – К.: КНТ, 2009. – 576 с.
29. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України: Монографія. – К.: «Текст», 2003. – 600 с.
30. Лопатин В.Н. Информационная безопасность России: Че¬ловек. Общество. Государство/Санкт-Петербургский универси¬тет МВД России. –СПб.: Фонд «Университет», 2010.– 428 с.
31. Ковалева Н.Н. Информационное право: учебное пособие.- М.: Дашков и К, 2008.-359 с.
32. Монойло А.В., Петренко А.И., Фролов О.Б. Государствен¬ная информационная политика в условиях информационно-пси¬хологической войны. – М.: Горячая линия. Телеком, 2013. – 541с.
33. Нашинець-Наумова А.Ю. Інформаційна безпека як складова частина національної безпеки України / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – № 8. – 2013. – С.63-67.
34. Нашинець-Наумова А.Ю. Информационная безопасность предприятия: теоретико-методологические основы правового обеспечения / А.Ю. Нашинець-Наумова // Адміністративне право і процес. – № 4(6). – 2013. – С.147-155.
35. Нашинець-Наумова А.Ю. Методологія «захищеного інформаційного розвитку» як парадигма інформаційної безпеки у XXI столітті / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – № 3. – 2014. –

С.54-58.

36. Нашинець-Наумова А.Ю. Система обеспечения информационной безопасности государства: организационно-правовые аспекты регулирования / А.Ю. Нашинець-Наумова // Legea şi viaţa: Revistă ştiinţifico-practică. – 9/2 (273). – 2014. – С. 106-111.

37. Новицький А.М. Правові основи формування інститутів інформаційного суспільства: теорія та практика: автореф. дис. на здобуття наук, ступеня доктора юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / А.М. Новицький. – Ірпінь, 2012. – 39 с.

38. Почепцов Г.Г. Информационные войны. – М.: «Руфлбук», К.: «Ваклер». – 2013. – 576 с.

39. Правові основи інформаційної діяльності: Навч. посібник / С.Ф. Гуцу. – Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін.-т», 2012. – 48 с.

40. Прокошева Т. Політика Міністерства культури і мистецтв в галузі створення та інтеграції інформаційних ресурсів українських бібліотек: За матеріалами дон. на Всеукр. наук.-практ. конф. // Бібл. планета. – 2000. – С. 2-5.

41. Швец Д.Ю. Информационная безопасность России и совре¬менные международные отношения. – М.: «Мир безопасности», 2014. – 176 с.

42. Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навч. посібник. – Х.: Консул, 2013. – 576 с.

43. Янина Е.В. Актуальные вопросы информационной безопасности: защита коммерческой тайны хозяйствующего субъекта в рамках локального нормативного акта / Е.В. Янина //Актуальные проблемы современной науки. – 2013. – № 2. – С.109- 111.

44. Ярачкин В.И. Информационная безопасность: Учеб. для студ. вузов, обуч. по гуманит. и соц.-экон. спец. – М.: Фонд «Мир», 2013. – 640 с.

## ПРО АВТОРІВ

**Лариса Борець –** кандидат юридичних наук, доцент кафедри інформаційного права та права інтелектуальної власності НТУУ «КПІ». Автор більш 50 наукових та навчально-методичних робіт.

В 1989 році закінчила Донецький інститут радянської торгівлі за спеціальністю «бухгалтерський облік та аналіз господарської діяльності» і здобула кваліфікацію економіста.

В 2000 році закінчила Донецький юридичний інститут внутрішніх справ при Донецькому національному університеті і здобула кваліфікацію юриста. На протязі 2000-2004 років поєднуючи практичну діяльність в правоохоронних органах навчалася за заочною формою навчання в ад'юнктурі Київського національного університету внутрішніх справ України.

У 2004 році захистила дисертацію за темою «Правове регулювання відомчого фінансового контролю в системі МВС України» за спеціальністю 12.00.07 «теорія управління; адміністративне право і процес; фінансове право; інформаційне право», у 2005 році присуджено науковий ступінь кандидата юридичних наук. В 2006 році отримала вчене звання доцента кафедри організації оперативно-розшукової діяльності.

**Анфіса Нашинець-Наумова** – кандидат юридичних наук, доцент кафедри правознавства Інституту суспільства Київського університету імені Бориса Грінченка. Автор більш 50 наукових та навчально-методичних робіт.

У 2002 р. – закінчила Національний педагогічний університет імені М.П. Драгоманова (присвоєна кваліфікація – «Викладач правознавства, юрист»).

У 2011 р. – захистила кандидатську дисертацію на тему: «Адміністративно-правове регулювання діяльності корпорацій в Україні» за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право», у 2011 році присуджено науковий ступінь кандидата юридичних наук.

**ДЛЯ НОТАТКІВ**

*Навчальне видання*

**БОРЕЦЬ Лариса Василівна**

**НАШИНЕЦЬ-НАУМОВА Анфіса Юріївна**

# ОСНОВИ ІНФОРМАЦІЙНОГО ПРАВА

**Навчальний посібник**

В авторській редакції

Технічний редактор *П.А. Діхтяр*
Коректор *О.А. Гусар*
Комп'ютерна верстка *А.В. Іванова*

Підп. до друку 15.10.14. Формат 60х84/16. Папір офс.
Офс. друк. Ум. друк. арк. 5,1. Обл.-вид. арк. 6,0.
Тираж 300 пр. Замовлення № 178-1. Вид. №46/1

Видавець і виготовлювач

Свідоцтво про внесення до Державного реєстру